

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

IN RE APPLICATION OF: Hideo SATO

GAU:

SERIAL NO: New Application

EXAMINER:

FILED: Herewith

FOR: ENCRYPTION APPARATUS

REQUEST FOR PRIORITY

COMMISSIONER FOR PATENTS
ALEXANDRIA, VIRGINIA 22313

SIR:

- ☐ Full benefit of the filing date of U.S. Application Serial Number _____, filed _____, is claimed pursuant to the provisions of 35 U.S.C. §120.
- ☐ Full benefit of the filing date(s) of U.S. Provisional Application(s) is claimed pursuant to the provisions of 35 U.S.C. §119(e):
Application No. _____ Date Filed _____

- ☒ Applicants claim any right to priority from any earlier filed applications to which they may be entitled pursuant to the provisions of 35 U.S.C. §119, as noted below.

In the matter of the above-identified application for patent, notice is hereby given that the applicants claim as priority:

COUNTRY

Japan

APPLICATION NUMBER

2002-241367

MONTH/DAY/YEAR

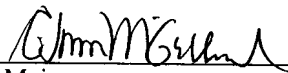
August 22, 2002

Certified copies of the corresponding Convention Application(s)

- ☒ are submitted herewith
- ☐ will be submitted prior to payment of the Final Fee
- ☐ were filed in prior application Serial No. _____ filed _____
- ☐ were submitted to the International Bureau in PCT Application Number _____
Receipt of the certified copies by the International Bureau in a timely manner under PCT Rule 17.1(a) has been acknowledged as evidenced by the attached PCT/IB/304.
- ☐ (A) Application Serial No.(s) were filed in prior application Serial No. _____ filed _____; and
- ☐ (B) Application Serial No.(s) _____
☐ are submitted herewith
- ☐ will be submitted prior to payment of the Final Fee

Respectfully Submitted,

OBLON, SPIVAK, McCLELLAND,
MAIER & NEUSTADT, P.C.



Gregory J. Maier

Registration No. 25,599

C. Irvin McClelland
Registration Number 21,124



22850

日 本 国 特 許 庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出 願 年 月 日

Date of Application:

2002年 8月22日

出 願 番 号

Application Number:

特願2002-241367

[ST.10/C]:

[JP2002-241367]

出 願 人

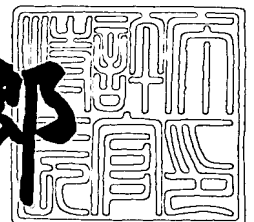
Applicant(s):

ソニー株式会社

2003年 6月10日

特 許 庁 長 官
Commissioner,
Japan Patent Office

太田信一郎



出証番号 出証特2003-3044936

【書類名】 特許願

【整理番号】 0290074001

【提出日】 平成14年 8月22日

【あて先】 特許庁長官 殿

【国際特許分類】 G09C 1/00

H04L 9/30

H04L 9/06

H04B 1/38

【発明者】

【住所又は居所】 東京都品川区北品川6丁目7番35号 ソニー株式会社
内

【氏名】 佐藤 英雄

【特許出願人】

【識別番号】 000002185

【氏名又は名称】 ソニー株式会社

【代理人】

【識別番号】 100110434

【弁理士】

【氏名又は名称】 佐藤 勝

【手数料の表示】

【予納台帳番号】 076186

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 0011610

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 暗号化装置

【特許請求の範囲】

【請求項 1】 公開鍵暗号化方式による暗号化処理を行う暗号化装置であって

公開鍵暗号化方式による暗号化処理を行う公開鍵暗号化処理手段と、

前記公開鍵暗号化処理手段によって用いるハッシュ値を生成するハッシュ値生成手段と、

前記ハッシュ値を格納する記憶手段とを備え、

少なくとも、前記ハッシュ値生成手段が前記記憶手段にアクセスするに際して、前記公開鍵暗号化処理手段における各種演算処理を制限すること
を特徴とする暗号化装置。

【請求項 2】 前記公開鍵暗号化処理手段は、演算用の値を保持するためのレジスタ及び結果を取り込むためのレジスタからなるレジスタ群を有し、

少なくとも、前記ハッシュ値生成手段における演算用の値を保持するためのレジスタ及び結果としてのハッシュ値を取り込むためのレジスタからなるレジスタ群を、前記公開鍵暗号化処理手段における前記レジスタ群と共用し、処理モードに応じて、動作させるハードウェアを時分割に切り替えること

を特徴とする請求項 1 記載の暗号化装置。

【請求項 3】 前記公開鍵暗号化処理手段によって暗号化処理を行う際に必要となる乱数を生成するために、共通鍵暗号化方式による暗号化処理を行う共通鍵暗号化処理手段を備え、

前記共通鍵暗号化処理手段におけるデータを保持するレジスタ及び鍵データを保持するレジスタからなるレジスタ群を、前記公開鍵暗号化処理手段における前記レジスタ群と共用すること

を特徴とする請求項 1 記載の暗号化装置。

【請求項 4】 前記共通鍵暗号化処理手段は、DES暗号化処理を行うこと
を特徴とする請求項 3 記載の暗号化装置。

【請求項 5】 前記公開鍵暗号化処理手段は、公開鍵暗号化方式による暗号化

処理に際する各種演算処理を行う公開鍵暗号化演算処理コア手段を有し、

前記ハッシュ値生成手段は、前記ハッシュ値の生成処理に際する各種演算処理を行うハッシュ値演算処理コア手段を有し、

前記公開鍵暗号化演算処理コア手段と、前記ハッシュ値演算処理コア手段とを共用すること

を特徴とする請求項 1 記載の暗号化装置。

【請求項 6】 前記公開鍵暗号化演算処理コア手段における加算手段と、前記ハッシュ値演算処理コア手段における加算手段とを共用すること

を特徴とする請求項 5 記載の暗号化装置。

【請求項 7】 前記公開鍵暗号化処理手段は、ビット幅を可変とするためのバス切り替えスイッチを有し、

前記ハッシュ値生成手段におけるバス切り替えスイッチを、前記公開鍵暗号化処理手段における前記バス切り替えスイッチと共用すること

を特徴とする請求項 1 記載の暗号化装置。

【請求項 8】 前記公開鍵暗号化処理手段によって暗号化処理を行う際に必要となる乱数を生成するために、共通鍵暗号化方式による暗号化処理を行う共通鍵暗号化処理手段を備え、

前記共通鍵暗号化処理手段におけるバス切り替えスイッチを、前記公開鍵暗号化処理手段における前記バス切り替えスイッチと共用すること

を特徴とする請求項 7 記載の暗号化装置。

【請求項 9】 前記ハッシュ値生成手段は、生成したハッシュ値を前記記憶手段に格納するに際して、前記公開鍵暗号化処理手段によって用いられるアドレスに該ハッシュ値を格納し、

前記公開鍵暗号化処理手段は、前記記憶手段に格納されたハッシュ値を読み出すこと

を特徴とする請求項 1 記載の暗号化装置。

【請求項 10】 前記公開鍵暗号化処理手段は、楕円曲線暗号化処理を行うこと

を特徴とする請求項 1 記載の暗号化装置。

【請求項 1 1】 前記ハッシュ値生成手段は、SHA-1 処理を行うことを特徴とする請求項 1 記載の暗号化装置。

【請求項 1 2】 通信機能を有する非接触型 IC カードに組み込まれていることを特徴とする請求項 1 記載の暗号化装置。

【発明の詳細な説明】

【0 0 0 1】

【発明の属する技術分野】

本発明は、いわゆる公開鍵暗号化方式による暗号化処理を行う暗号化装置に関する。

【0 0 0 2】

【従来の技術】

近年、例えば、いわゆるインターネット等を利用した電子商取引やオンラインショッピングといった各種通信技術を利用した様々なサービスが普及しつつある。また、近年では、通信技術の進歩にともない、端末を介した通信技術のみならず、例えば、交通機関の料金徴収やいわゆる電子マネー等に利用するための通信機能を集積回路化した非接触型半導体メモリカードといったカード状のデバイスも開発されている。

【0 0 0 3】

このような通信機能を有するカード状のデバイス（以下、非接触型 IC（Integrated Circuit）カードという。）は、取り扱いの便宜等の観点から、少ない回路規模で構成されるとともに、極めて少ない電力消費で動作することができ、且つ高速な処理を行うことが求められる。

【0 0 0 4】

【発明が解決しようとする課題】

ところで、上述した非接触型 IC カードを用いたサービスにおいては、通常、通信相手の正当性を認証するための相互認証処理や、データ通信の安全性を確保するための暗号化処理が行われる。その際、非接触型 IC カードにおいては、処理の高速化が要求されることから、これらの機能をソフトウェアによって実装す

ると、高いクロックのCPU (Central Processing Unit) を要することとなり、実用的でない。そのため、非接触型ICカードにおいては、これらの機能をソフトウェアによって実装するのではなく、ハードウェアによって実装するのが望ましい。

【0005】

ここで、このようなハードウェアによって上述した機能を実装する非接触型ICカードにおいては、電力消費を極力抑制するために、例えばいわゆるDES (Data Encryption Standard) 暗号化方式といった比較的少ない回路規模及び電力消費で実装することができるいわゆる共通鍵暗号化方式を採用するものが多かった。

【0006】

しかしながら、暗号化及び復号に共通の鍵を用いる共通鍵暗号化方式は、鍵データの授受を行う必要があるといった観点から、不正な第三者による攻撃に弱いという問題がある。そのため、非接触型ICカードにおいては、将来的に金融サービスに適用する場合等の問題が懸念されていた。

【0007】

そのため、非接触型ICカードを用いたサービスにおいては、非接触型ICカードとして、例えばいわゆるRSA (Rivest-Shamir-Adleman) 暗号化方式や楕円曲線暗号化方式 (Elliptic Curve Cryptosystem; ECC) といったように、暗号化と復号とに用いる鍵を異なるものとし、秘密に保つ必要がある共通鍵を特定の1人が持てばよいいわゆる公開鍵暗号化方式を採用したセキュリティの高いシステムが要求されつつあり、公開鍵を用いた署名生成及び署名検証を行う非接触型ICカードの開発も多く試みられている。

【0008】

しかしながら、公開鍵暗号化方式は、共通鍵暗号化方式に比べ、セキュリティ性が極めて向上するものの、演算量が非常に膨大となることから、これをハードウェアによって実装する際には、回路規模が数十倍に増大し、規模が増大した回路に供給する電力も必然的に増大することになる。特に、各演算処理が同時に行われた場合には、これら演算処理が行われる回路で消費される瞬時電力の増大を

招く。

【 0 0 0 9 】

そのため、このような公開鍵暗号化方式を採用した非接触型 I C カードにおいては、回路規模、消費電力、及びコストの面で十分な特性を得ることができなかった。特に、非接触型 I C カードにおいては、限られた電力の多くを、暗号化処理を行うための回路に供給する必要がある、通信距離が数ミリ程度と短いものしか実用化されていない実情である。さらに、瞬時電力が予め制限された電力を上回った場合には各種演算処理が停止し、再度演算処理がやり直されることとなり、非接触型 I C カードにおける処理の遅延化を招く問題も生じている。

【 0 0 1 0 】

図 1 4 は、縦軸を消費電力 W 、横軸を処理時刻 T とし、各処理における消費電力、及びこれら消費電力が加算された非接触型 I C カード全体における消費電力を模式的に比較した図である。同図 (A) 乃至 (C) は、ゲート、算出されたハッシュ値が格納される A L U - R A M、及び R A M のそれぞれにおける処理に際して消費される消費電力を個別に示した図であり、同図 (D) はこれら各処理における消費電力を加算した該非接触型 I C カード全体の消費電力を示す図である。同図 (A) 乃至 (C) によれば、処理時刻 t_0 において、ゲート、A L U R A M、及び R A M において同時に処理動作が行われ、これら各処理における消費電力が加算された該非接触型 I C カード全体の消費電力は、同図 (D) に示すように制限電力を瞬間的に超える場合がある。非接触型 I C カード全体としての消費電力が制限電力を超えると、各種処理動作を停止した後、再度処理動作が行われることとなり、消費電力が制限電力を超える時点までに行われた各種処理が無駄なものとなる。

【 0 0 1 1 】

さらに、消費電力が制限電力を超える毎に再度処理動作が行われると、該非接触型 I C カードにおける処理を高速で行うことが難しくなり、各種処理を高速で行うことを求められる非接触型 I C カードでは重大な問題となる。特に、A L U R A M にアクセスするに際しては、 $2 \sim 3 \text{ n s e c}$ の如き短時間に消費される瞬時電力が大きく、これと同時に他の処理動作が行われると非接触型 I C カード

全体の瞬時電力が制限電力を超え、各種処理動作に遅延が生じる。

【 0 0 1 2 】

このように、非接触型 I C カードにおいては、セキュリティの面で強固であり公開鍵暗号化方式を採用することが期待されているものの、供給可能な電力やチップサイズ等の制限があるだけでなく、実装することが極めて困難であるうえ、消費電力の制限により高速処理を行うことが困難であった。

【 0 0 1 3 】

よって、本発明は、このような実情に鑑みてなされたものであり、回路規模を削減し、瞬時電力が低減された状態のもとに高速且つ安全に公開鍵を用いた署名生成及び署名検証を可能とする暗号化装置を提供することを目的とする。

【 0 0 1 4 】

【課題を解決するための手段】

上述した目的を達成する本発明にかかる暗号化装置は、公開鍵暗号化方式による暗号化処理を行う暗号化装置であって、公開鍵暗号化方式による暗号化処理を行う公開鍵暗号化処理手段と、公開鍵暗号化処理手段によって用いるハッシュ値を生成するハッシュ値生成手段と、ハッシュ値を格納する記憶手段とを備え、少なくとも、ハッシュ値生成手段が記憶手段にアクセスするに際して、公開鍵暗号化処理手段における各種演算処理を制限することを特徴としている。消費電力が比較的大きい処理動作を行うに際して、他の動作を一時的に制限することにより瞬時電力を低減し、電力を限界値以下に消費電力を抑制することにより、各種処理動作を停止させることなく高速処理を行うことができる。

【 0 0 1 5 】

このような本発明にかかる暗号化装置においては、公開鍵暗号化処理手段が、演算用の値を保持するためのレジスタ及び結果を取り込むためのレジスタからなるレジスタ群を有し、少なくとも、ハッシュ値生成手段における演算用の値を保持するためのレジスタ及び結果としてのハッシュ値を取り込むためのレジスタからなるレジスタ群を、公開鍵暗号化処理手段におけるレジスタ群と共用し、処理モードに応じて、動作させるハードウェアを時分割に切り替える。従って、各種処理動作を行うハードウェアを時分割で動作させることにより、瞬時電力を低減

することができ、消費電力が制限電力を超えることにより処理動作が停止させられることがなく、高速処理を行うことが可能となる。

【 0 0 1 6 】

また、この本発明にかかる暗号化装置においては、公開鍵暗号化処理手段によって暗号化処理を行う際に必要となる乱数を生成するために、共通鍵暗号化方式による暗号化処理を行う共通鍵暗号化処理手段を備え、共通鍵暗号化処理手段におけるデータを保持するレジスタ及び鍵データを保持するレジスタからなるレジスタ群を、公開鍵暗号化処理手段におけるレジスタ群と共用する。

【 0 0 1 7 】

このような本発明にかかる暗号化装置においては、公開鍵暗号化処理手段が、公開鍵暗号化方式による暗号化処理に際する各種演算処理を行う公開鍵暗号化演算処理コア手段を有し、ハッシュ値生成手段は、ハッシュ値の生成処理に際する各種演算処理を行うハッシュ値演算処理コア手段を有し、公開鍵暗号化演算処理コア手段と、ハッシュ値演算処理コア手段とを共用する。

【 0 0 1 8 】

さらに、この本発明にかかる暗号化装置において、公開鍵暗号化演算処理コア手段における加算手段と、ハッシュ値演算処理コア手段における加算手段とを共用する。

【 0 0 1 9 】

このような本発明にかかる暗号化装置は、公開鍵暗号化処理手段は、ビット幅を可変とするためのバス切り替えスイッチを有し、ハッシュ値生成手段におけるバス切り替えスイッチを、公開鍵暗号化処理手段におけるバス切り替えスイッチと共用する。

【 0 0 2 0 】

さらにまた、この本発明にかかる暗号化装置において、公開鍵暗号化処理手段によって暗号化処理を行う際に必要となる乱数を生成するために、共通鍵暗号化方式による暗号化処理を行う共通鍵暗号化処理手段を備え、共通鍵暗号化処理手段におけるバス切り替えスイッチを、公開鍵暗号化処理手段におけるバス切り替えスイッチと共用する。

【 0 0 2 1 】

このような本発明にかかる暗号化装置は、ハッシュ値生成手段は、生成したハッシュ値を記憶手段に格納するに際して、公開鍵暗号化処理手段によって用いられるアドレスに該ハッシュ値を格納し、公開鍵暗号化処理手段は、記憶手段に格納されたハッシュ値を読み出す。

【 0 0 2 2 】

このような本発明にかかる暗号化装置は、共通鍵暗号化処理手段を備える場合には、公開鍵暗号化処理手段による暗号化処理とハッシュ値生成手段によるハッシュ値生成処理との間のみならず、この共通鍵暗号化処理手段による暗号化処理との間でも、バス切り替えスイッチを時分割共用する。

【 0 0 2 3 】

このような本発明にかかる暗号化装置は、ハッシュ値生成手段によって生成されたハッシュ値を、公開鍵暗号化処理手段による次回の暗号化処理にて用いるためにデータ転送することなく、記憶手段を介して受け渡す。

【 0 0 2 4 】

【発明の実施の形態】

以下、本発明を適用した具体的な実施の形態について図面を参照しながら詳細に説明する。

【 0 0 2 5 】

この実施の形態は、例えば、通信機能を集積回路化した非接触型半導体メモリカードといったカード状のデバイス（以下、非接触型 I C (Integrated Circuit) カードという。）等に適用することができるものであって、通信相手の正当性を認証するための相互認証処理や、データ通信の安全性を確保するための暗号化処理の機能を、ハードウェアによって実装した暗号化装置である。特に、この暗号化装置は、いわゆる公開鍵暗号化方式を採用するものであって、暗号処理を行うに際して生成されるハッシュ値を記憶させるときに、瞬時電力の増大を招くことがないようにその他の各種処理を制限し、瞬時電力が低減された状態のもとに高速且つ安全に公開鍵を用いた署名生成及び署名検証を可能とするものである。

【 0 0 2 6 】

さらに、各種処理を行うための各ハードウェアを当該各種処理間で共用して時分割処理を行うことにより、瞬時電力を低減することができるとともに、回路規模を削減して極めて少ない電力消費のもとに高速且つ安全に公開鍵を用いた署名生成及び署名検証を可能とするものである。

【 0 0 2 7 】

なお、以下では、説明の便宜上、暗号化装置は、公開鍵暗号化方式として、いわゆる楕円曲線暗号化方式 (Elliptic Curve Cryptosystem; ECC) を採用し、認証やデジタル署名等に用いるハッシュ関数として、いわゆる SHA-1 (Secure Hash Algorithm-1) を用い、さらに、暗号化処理を行う際に必要となる鍵生成の過程等において用いる乱数を、共通鍵暗号化方式の 1 つであるいわゆる DES (Data Encryption Standard) 暗号化方式を用いて生成するものとして説明する。すなわち、暗号化装置は、公開鍵暗号化方式の一連の信号処理として、少なくとも、これら楕円曲線暗号化処理、SHA-1 処理、及び DES 暗号化処理を行うものとして説明する。

【 0 0 2 8 】

まず、暗号化装置において、楕円曲線暗号化処理、SHA-1 処理、及び DES 暗号化処理を時分割で行うに際して各ハードウェアを共用するための概念について説明する。

【 0 0 2 9 】

まず、暗号化装置においては、楕円曲線暗号化処理、SHA-1 処理、及び DES 暗号化処理のそれぞれを行うためのハードウェア構成要素としてのレジスタを共用する。すなわち、楕円曲線暗号化処理を行う暗号化エンジンにおけるハードウェア構成要素は、機能分析的に分解すると、図 1 (A) に概念を示すように、レジスタ群と楕円曲線演算処理コア回路とに大別することができ、レジスタ群が当該ハードウェア構成要素の半分程度を占める。また、SHA-1 処理を行う暗号化エンジンにおけるハードウェア構成要素についても、機能分析的に分解すると、同図 (B) に示すように、レジスタ群と SHA-1 演算処理コア回路とに大別することができる。そこで、暗号化装置においては、同図 (C) に示すように、楕円曲線暗号化処理及び SHA-1 処理のそれぞれを行うためのハードウェア

ア構成要素としてのレジスタを共用する。さらに、DES暗号化処理を行う暗号化エンジンにおけるハードウェア構成要素についても、機能分析的に分解すると、図示しないが、レジスタ群とDES演算処理コア回路とに大別することができることから、暗号化装置においては、楕円曲線暗号化処理及びSHA-1処理に加え、DES暗号化処理を行うためのハードウェア構成要素としてのレジスタをも共用する。これにより、暗号化装置は、回路規模の削減を図ることが可能となる。

【0030】

また、暗号化装置においては、SHA-1処理を行うための演算処理コア回路と楕円曲線暗号化処理を行う演算処理コア回路とを共用する。すなわち、ハッシュ値を算出するSHA-1処理においては、高速に動作する加算器が設けられた演算処理コア回路が必要とされる。また、楕円曲線暗号化処理においても、演算処理コア回路に加算器が設けられる。そこで、暗号化装置においては、SHA-1処理を行うための演算処理コア回路と楕円曲線暗号化処理を行う演算処理コア回路とにおける加算器等のゲート数が多いハードウェア構成要素を共用する。これにより、暗号化装置は、回路規模の削減を図ることが可能となる。

【0031】

さらに、暗号化装置においては、暗号化エンジンにおけるバス切り替えスイッチ群とその他各種機能の切り替えスイッチとを共用する。すなわち、公開鍵暗号化方式における鍵長を可変とするためにはバスを切り替える必要があることから、楕円曲線暗号化処理を行う暗号化エンジンには、例えば32ビット幅のスイッチが多数設けられる。これらのスイッチは、その構成上、SHA-1処理やDES暗号化処理を行うハードウェアにおいても共用可能である。そこで、暗号化装置においては、これらバス切り替えスイッチ群を、その他各種機能の切り替えスイッチとして流用する。これにより、暗号化装置は、回路規模の削減を図ることが可能となる。

【0032】

さらにまた、暗号化装置においては、レジスタやメモリ等のハードウェアを時分割共用する。すなわち、暗号化装置における公開鍵暗号化方式の信号処理は、

D E S 暗号化処理を用いた乱数の生成、S H A - 1 処理によるハッシュ値の算出、及び楕円曲線暗号化処理における楕円曲線の算出に大別される。しかしながら、これらの処理は、同時には行うことができないものであることから、ハードウェアを共用する場合には必然的に時分割処理を行うことになる。そこで、暗号化装置においては、これを利用して、レジスタやメモリ等のハードウェアを各処理で時分割共用する。これにより、暗号化装置は、回路規模の削減と電力消費の削減とを図ることが可能となる。

【 0 0 3 3 】

このように、暗号化装置は、楕円曲線暗号化処理、S H A - 1 処理、及びD E S 暗号化処理を行うための各ハードウェアを共用し、時分割処理を行うものとして構成される。

【 0 0 3 4 】

さて、暗号化装置においては、具体的に実装するにあたって、各ハードウェアを共用するために、楕円曲線暗号化処理、S H A - 1 処理、及びD E S 暗号化処理を行うための各ハードウェアを共用しやすい構成にする必要がある。以下では、これらの楕円曲線暗号化処理、S H A - 1 処理、及びD E S 暗号化処理を行うための各ハードウェアを共用しやすい構成とした具体的な実装例について説明した後、これらの各ハードウェアを統合した具体的な暗号化装置の実装例について説明する。

【 0 0 3 5 】

まず、S H A - 1 処理を行うためのハードウェアである S H A - 1 処理回路について説明する。

【 0 0 3 6 】

S H A - 1 処理回路は、S H A - 1 処理を行うものである。S H A - 1 とは、認証やデジタル署名等に用いられるハッシュ関数の1つであり、512ビットの任意の原文から160ビットの擬似乱数であるハッシュ値を発生する不可逆な一方向性関数である。S H A - 1 は、原文が1ビットでも異なる場合には、全く異なるハッシュ値を出力することから、ハッシュ値を生成して通信経路の両端で比較することにより、通信途中で原文が改竄されたか否かを検出する用途に広く

用いられる。具体的には、SHA-1を用いたSHA-1処理においては、あるメッセージを送信する場合には、送信側がメッセージとこのメッセージに対するハッシュ値とを同時に送信し、受信側では受け取ったメッセージからハッシュ値を算出し、その結果得られたハッシュ値と送信側から送信されたハッシュ値とを比較することにより、データの改竄の有無を検証することができる。SHA-1処理回路は、このようなSHA-1処理を行うものとして構成されるが、ここでは、いわゆるFIPS (Federal Information Processing Standard) に規定されているSHA-1のうち、回路規模が比較的小さくて済む"ALTERNATIVE METHOD"を採用する。

【0037】

この"ALTERNATIVE METHOD"のアルゴリズムは、通常であれば80個の32ビット・ワード配列 $W(0), \dots, W(79)$ を用いて行うSHA-1処理を少ないメモリ空間で実現するための代替手段であり、 $\{W(t)\}$ を循環キューとみなし、16個の32ビット・ワード配列 $W(0), \dots, W(15)$ を用いて行うものである。このアルゴリズムにおいては、512ビット長のブロック $M(i)$ 毎に、以下の4つの工程が行われる。なお、以下における値MASKは、16進数で0000000Fとする。

【0038】

まず、このアルゴリズムにおいては、第1の工程として、ブロック $M(i)$ を16個のワード $W(0), \dots, W(15)$ に分割する。なお、ワード $W(0)$ は、最も左側のワードである。

【0039】

続いて、このアルゴリズムにおいては、はじめの5つのワードバッファを、それぞれ、A, B, C, D, Eとし、次の5つのワードバッファを、それぞれ、H0, H1, H2, H3, H4とすると、第2の工程として、次式(1)に示す演算を行う。

【0040】

【数 1】

$$\begin{cases} A = H0; \\ B = H1; \\ C = H2; \\ D = H3; \\ E = H4; \end{cases} \dots (1)$$

【0 0 4 1】

続いて、このアルゴリズムにおいては、第 3 の工程として、変数 t を "0" から "7 9" まで変化させ、次式 (2) に示す演算を行う。

【0 0 4 2】

【数 2】

$$\begin{cases} s = t \text{ AND } MASK; \\ \text{if } (t \geq 16) \\ W[s] = S1(W[(s+13) \text{ AND } MASK] \text{ XOR } W[(s+8) \text{ AND } MASK] \\ \quad \quad \quad \text{XOR } W[(s+2) \text{ AND } MASK] \text{ XOR } W[s]); \\ TEMP = S5(A) + F(t; B, C, D) + E + W[s] + Kt; \\ E = D; \\ D = C; \\ C = S30(B); \\ B = A; \\ A = TEMP; \end{cases} \dots (2)$$

【0 0 4 3】

なお、上式 (2) における $S_n(X)$ は、 X をワード値、 n を $0 \leq n < 32$ の整数としたときの循環左シフト操作を表すものである。また、上式 (2) における $F(t; B, C, D)$ は、次式 (3) に示す関数であり、 $K(t)$ は、次式 (4) に示す 16 進数のワード定数列である。

【 0 0 4 4 】

【数 3】

$$\begin{cases} F(t; B, C, D) = (B \text{ AND } C) \text{ OR } ((\text{NOT } B) \text{ AND } D) & (0 \leq t \leq 19) \\ F(t; B, C, D) = B \text{ XOR } C \text{ XOR } D & (20 \leq t \leq 39) \\ F(t; B, C, D) = (B \text{ AND } C) \text{ OR } (B \text{ AND } D) \text{ OR } (C \text{ AND } D) & (40 \leq t \leq 59) \\ F(t; B, C, D) = B \text{ XOR } C \text{ XOR } D & (60 \leq t \leq 79) \end{cases} \dots (3)$$

【 0 0 4 5 】

【数 4】

$$\begin{cases} K(t) = 5A827999 & (0 \leq t \leq 19) \\ K(t) = 6ED9EBA1 & (20 \leq t \leq 39) \\ K(t) = 8F1BBCDC & (40 \leq t \leq 59) \\ K(t) = CA62C1D6 & (60 \leq t \leq 79) \end{cases} \dots (4)$$

【 0 0 4 6 】

そして、このアルゴリズムにおいては、第 4 の工程として、次式 (5) に示す演算を行い、一連の処理を終了する。

【 0 0 4 7 】

【数 5】

$$\begin{cases} H0 = H0 + A; \\ H1 = H1 + B; \\ H2 = H2 + C; \\ H3 = H3 + D; \\ H4 = H4 + E; \end{cases} \dots (5)$$

【 0 0 4 8 】

ここで、このような "ALTERNATIVE METHOD" のアルゴリズムを一般的な形式で実

装すると、SHA-1 処理回路は、図 2 に示すような構成となる。

【0049】

すなわち、SHA-1 処理回路は、同図に示すように、図示しない CPU (Central Processing Unit) から供給される演算用の値をテンポラリに保持するシフトレジスタ群 10 と、上述したワードバッファ A, B, C, D, E としての 5 つのシフトレジスタと上述した値 TEMP を保持するシフトレジスタとからなり結果としてのハッシュ値を取り込むためのシフトレジスタ群 20 と、初期値 H0, H1, H2, H3, H4 及び上式 (4) に示した 16 進数のワード定数列 K (t) を保持する ROM (Read Only Memory) 30 と、結果としてのハッシュ値を格納する ALU RAM (Arithmetic and Logical Unit Random Access Memory) 40 とを備えるとともに、上述したアルゴリズムにおける各種演算を行うための各種演算処理回路を備える。なお、同図における MUX0, MUX3, MUX4, MUX5 は、それぞれ、バス切り替えスイッチである。

【0050】

ここで、SHA-1 処理回路においては、回路規模を考慮すると、上式 (2) 中、値 TEMP の算出式、すなわち、次式 (6) に示す演算を実行する 32 ビット 5 入力の加算器が最も回路規模の増大を招来する要因となる。そこで、SHA-1 処理回路としては、楕円曲線暗号化処理の演算時間に比べて SHA-1 処理の演算時間が無視できるほど短いことを利用して、図 3 に示すように、32 ビット 2 入力の加算器を 4 回用いることにより、回路規模を削減することが可能となる。

【0051】

【数 6】

$$TEMP = SS(A) + F(t; B, C, D) + E + W[s] + Kt; \quad \dots (6)$$

【0052】

この場合、SHA-1 処理回路においては、図 2 に示した構成の場合に比べ、演算時間が約 4 ～ 5 倍程度になるものの、楕円曲線暗号化処理の演算時間に比べれば十分短時間であることから、実用上は何らの支障も招来せず、サイズが膨大

なデータやストリームに対して S H A - 1 処理を施すような特殊な場合を除けば、十分な性能を得ることが可能である。

【 0 0 5 3 】

なお、S H A - 1 処理回路においては、後述するように、楕円曲線暗号化処理の際に使用する加算器と兼用することにより、当該 S H A - 1 処理回路における加算器そのものが不要となることから、さらに大幅な回路規模の削減を図ることが可能となる。

【 0 0 5 4 】

また、S H A - 1 処理回路においては、上式 (2) 中、ワード $W[s]$ の算出式、すなわち、次式 (7) に示す演算を実行する際に、必ず 3 2 ビット \times 1 6 段のシフトレジスタが必要となることがわかる。

【 0 0 5 5 】

【数 7】

$$\begin{aligned} W[s] = & S1(W[(s+13) \text{ AND } MASK] \text{ XOR } W[(s+8) \text{ AND } MASK] \\ & \text{ XOR } W[(s+2) \text{ AND } MASK] \text{ XOR } W[s]); \\ & \dots (7) \end{aligned}$$

【 0 0 5 6 】

さらに、S H A - 1 処理回路においては、上式 (2) 中、ワードバッファ A, B, C, D, E の算出式、すなわち、次式 (8) に示す演算を実行する際にも、少なくとも 3 2 ビット \times 5 ~ 6 段のシフトレジスタが必要となる。

【 0 0 5 7 】

【数 8】

$$\begin{cases} E = D; \\ D = C; \\ C = S30(B); \\ B = A; \\ A = TEMP; \end{cases} \dots (8)$$

【 0 0 5 8 】

ここで、楕円曲線暗号化処理を行うためのハードウェアである楕円曲線暗号化

処理回路においては、後述するように、段数が可変とされる 32 ビット×7 段のシフトレジスタ群が 3 組設けられることから、SHA-1 処理回路においては、これらのシフトレジスタを流用することにより、当該 SHA-1 処理回路に専用のシフトレジスタを設ける必要がなくなり、さらに大幅な回路規模の削減を図ることが可能となる。結果的に、暗号化装置においては、通常であれば 60000 ゲート以上からなる SHA-1 処理回路を、楕円曲線暗号化処理回路に対して 2000 ゲート程度の追加回路のみで実現することができる。

【0059】

さて、このような SHA-1 処理回路は、図 4 及び図 5 に示すような一連の工程を経ることにより、基本動作を行う。なお、ここでは、先に図 2 に示した構成からなる SHA-1 処理回路の基本動作について説明する。

【0060】

まず、SHA-1 処理回路は、図 4 に示すように、ステップ S1 において、変数 t を“0”とする。

【0061】

続いて、SHA-1 処理回路は、ステップ S2 において、シフトレジスタ群 10 における各シフトレジスタに対して、パディングされたデータのうち、32×16 ブロック (= 512 ビット) からなる先頭のデータをロードする。

【0062】

続いて、SHA-1 処理回路は、ステップ S3 において、バス切り替えスイッチ MUX0 を、演算処理回路 W[s] の出力側に切り替える。

【0063】

続いて、SHA-1 処理回路は、ステップ S4 において、初期値 H0, H1, H2, H3, H4 を ROM30 から読み出し、バス切り替えスイッチ MUX4、加算器、及びシフトレジスタ群 20 における値 TEMP を保持するシフトレジスタを介して、シフトレジスタ群 20 におけるワードバッファ A, B, C, D, E としての各シフトレジスタに対して順次ロードする。

【0064】

続いて、SHA-1 処理回路は、ステップ S5 において、値 TEMP としてオ

ールゼロをセットする。

【 0 0 6 5 】

続いて、SHA-1 処理回路は、ステップ S 6 において、バス切り替えスイッチ MUX 5 を制御して、次式 (9) に示すように、加算器によって 4 回に分けた加算処理を行うことにより、上式 (6) に示した演算と等価な演算を行い、値 TEMP を算出する。

【 0 0 6 6 】

【 数 9 】

$$\left\{ \begin{array}{l} S5(A) + F(t) \Rightarrow TEMP; \\ TEMP + E \Rightarrow TEMP; \\ TEMP + W[s] \Rightarrow TEMP; \\ TEMP + K(t) \Rightarrow TEMP; \end{array} \right. \quad \dots (9)$$

【 0 0 6 7 】

続いて、SHA-1 処理回路は、ステップ S 7 において、バス切り替えスイッチ MUX 3 を、演算処理回路 S 3 0 の出力側に切り替え、各シフトレジスタに保持されている値 TEMP, A, B, C, D, E を、それぞれ、1 クロック分だけ右にシフトする。これにより、SHA-1 処理回路は、上式 (8) に示した各値を得ることができる。

【 0 0 6 8 】

続いて、SHA-1 処理回路は、ステップ S 8 において、シフトレジスタ群 1 0 における各シフトレジスタに保持されている値を、それぞれ、1 クロック分だけ右にシフトする。

【 0 0 6 9 】

続いて、SHA-1 処理回路は、ステップ S 9 において、変数 t が "7 9" に到達したか否かを判定する。ここで、SHA-1 処理回路は、変数 t が "7 9" に到達していないものと判定した場合には、ステップ S 1 0 へと処理を移行し、変数 t を "1" だけインクリメントした後、ステップ S 2 乃至ステップ S 8 の処理を繰り返す。すなわち、SHA-1 処理回路は、ステップ S 2 乃至ステップ S 8 の処理を、変数 t を "0" から "7 9" まで変化させて行う。

【 0 0 7 0 】

一方、SHA-1 処理回路は、変数 t が "79" に到達したものと判定した場合には、ステップ S 1 1 へと処理を移行し、バス切り替えスイッチ MUX 3 を、演算処理回路 S 3 0 の出力側とは反対側に切り替えるとともに、バス切り替えスイッチ MUX 4 を、ROM 3 0 の出力側に切り替え、さらに、バス切り替えスイッチ MUX 5 の出力をワードバッファ E としてのシフトレジスタからの出力とすることにより、ワードバッファ A, B, C, D, E としての各シフトレジスタに保持されている値に対して、それぞれ、初期値 H_0, H_1, H_2, H_3, H_4 を加算器によって加算する。

【 0 0 7 1 】

続いて、SHA-1 処理回路は、ステップ S 1 1 における加算器による演算結果が、値 TEMP を保持するシフトレジスタに供給されることから、ステップ S 1 2 において、上式 (5) の演算を実現するように、各シフトレジスタに保持されている値を、それぞれ、6 クロック分だけ右にシフトする。

【 0 0 7 2 】

そして、SHA-1 処理回路は、図 5 に示すように、ステップ S 1 3 において、ワードバッファ A, B, C, D, E としての各シフトレジスタに保持されている値を、それぞれ、ALU RAM 4 0 に格納する。

【 0 0 7 3 】

続いて、SHA-1 処理回路は、ステップ S 1 4 において、パディングの結果が 5 1 2 ビットであるか否かを判定する。

【 0 0 7 4 】

ここで、SHA-1 処理回路は、パディングの結果が 5 1 2 ビットであるものと判定した場合には、ステップ S 1 3 において ALU RAM 4 0 に格納された値が、最終的なハッシュ値となることから、そのまま一連の処理を終了する。

【 0 0 7 5 】

一方、SHA-1 処理回路は、パディングの結果が 5 1 2 ビットでない、すなわち、5 1 2 ビットを超えるものと判定した場合には、ステップ S 1 5 において、パディングしたデータが全てシフトレジスタ群 1 0 における各シフトレジスタ

に対してロードされて処理が終了したか否かを判定する。

【 0 0 7 6 】

ここで、SHA-1 処理回路は、パディングしたデータが全てシフトレジスタ群 1 0 における各シフトレジスタに対してロードされておらず処理が終了していないものと判定した場合には、ステップ S 1 6 において、ステップ S 1 3 における状態を保持しつつ、次の 5 1 2 ビットのデータをシフトレジスタ群 1 0 における各シフトレジスタに対してロードする。

【 0 0 7 7 】

続いて、SHA-1 処理回路は、ステップ S 1 7 において、バス切り替えスイッチ MUX 4 を、ALU RAM 4 0 の出力側に切り替え、ステップ S 1 3 において ALU RAM 4 0 に格納された値を、それぞれ、ワードバッファ A, B, C, D, E としての各シフトレジスタに対してロードする。

【 0 0 7 8 】

続いて、SHA-1 処理回路は、ステップ S 1 8 において、バス切り替えスイッチ MUX 0 を、演算処理回路 W [s] の出力側に切り替え、図 4 中ステップ S 5 からの処理を繰り返す。

【 0 0 7 9 】

そして、SHA-1 処理回路は、ステップ S 1 5 における判定の結果、パディングしたデータが全てシフトレジスタ群 1 0 における各シフトレジスタに対してロードされて処理が終了したものと判定した場合には、ステップ S 1 3 において ALU RAM 4 0 に格納された値が、最終的なハッシュ値となることから、そのまま一連の処理を終了する。

【 0 0 8 0 】

SHA-1 処理回路は、このような一連の処理を行うことにより、ハッシュ値を生成する。

【 0 0 8 1 】

つぎに、楕円曲線暗号化処理を行うためのハードウェアである楕円曲線暗号化処理回路について説明する。

【 0 0 8 2 】

楕円曲線暗号化処理回路は、楕円曲線暗号化処理を行うものである。楕円曲線暗号化とは、暗号化と復号とに異なる通信鍵を用いる公開鍵暗号化アルゴリズムの1つであり、160ビット長の鍵を用いることにより、1024ビット長の鍵を用いたいわゆるRSA (Rivest-Shamir-Adleman) 暗号化方式と同等の性能を発揮する暗号化方式である。暗号化装置において、楕円曲線暗号化処理回路は、いわゆるモンゴメリー (Montgomery) 法を用いて構成される。すなわち、楕円曲線暗号化処理回路は、図6に示すように、図示しないCPUから供給される演算用の値をテンポラリに保持する32ビット幅のシフトレジスタ群50、60と、結果を取り込むためのシフトレジスタ群70と、主に32ビット幅の入力を有する図示しない加算器、減算器、及び乗算器を内部に有する楕円曲線演算処理コア回路80とを備える。なお、同図におけるMUX0、MUX1、MUX2は、それぞれ、バス切り替えスイッチである。

【0083】

このような楕円曲線暗号化処理回路においては、モンゴメリー法と称される特殊な手法を用いて処理の高速化及び回路規模の削減を実現する。モンゴメリー法による楕円曲線演算処理コア回路80は、主に、加算器、減算器、及び乗算器の組み合わせ回路によって構成され、演算のステップ毎に32ビット幅のデータ同士の処理を行う。そこで、暗号化装置においては、回路規模の削減を図るために、上述したように、楕円曲線演算処理コア回路80の内部に設けられる加算器を、SHA-1処理回路における加算器と共用する。

【0084】

さらに、モンゴメリー法による楕円曲線演算処理コア回路80と、これと共用されるSHA-1処理回路を構成する乗算器による処理においては、加算器及び減算器が処理に要する処理時間に比べて乗算器が処理に要する処理時間は大きい。従って、これに伴う処理の遅延は、ゲートにおいて消費される消費電力が鋭いピークを持つことを抑制し、ゲートにおける瞬時電力を低減することが可能となる。

【0085】

また、楕円曲線暗号化処理回路においては、3組の32ビット幅のシフトレジ

スタ群 5 0, 6 0, 7 0 が設けられるが、例えば 1 6 0 ビット幅、1 9 2 ビット幅、又は 2 2 4 ビット幅にも対応するために、各シフトレジスタ群 5 0, 6 0, 7 0 のそれぞれに対応して、ビット幅を可変とするためのバス切り替えスイッチ MUX 0, MUX 1, MUX 2 が設けられる。すなわち、楕円曲線暗号化処理回路においては、1 6 0 ビット幅、1 9 2 ビット幅、又は 2 2 4 ビット幅にも対応するために、3 組の 3 2 ビット幅のシフトレジスタ群 5 0, 6 0, 7 0 が、それぞれ、5, 6, 7 段に切り替え可能に構成される。

【 0 0 8 6 】

この具体例としては、図 7 (A) にシフトレジスタ群 6 0 の近傍の要部構成を示すように、入力と、5 段目、6 段目、及び 7 段目のシフトレジスタのそれぞれからの出力とのうち、いずれか 1 つの信号を、バス切り替えスイッチ MUX 1 からの出力とするように、シフトレジスタ群 6 0 における各シフトレジスタのうち、右側のシフトレジスタから個数を可変とするものが考えられる。また、他の具体例としては、図 7 (B) にシフトレジスタ群 6 0 の近傍の要部構成を示すように、入力と、7 段目のシフトレジスタのそれぞれからの出力とのうち、いずれか 1 つの信号を出力とするバス切り替えスイッチ MUX 1 を設けるとともに、1 段目のシフトレジスタの後段にバス切り替えスイッチ MUX 2 を設け、さらに、2 段目のシフトレジスタの後段にバス切り替えスイッチ MUX 3 を設けるといったように、シフトレジスタ群 6 0 における各シフトレジスタのうち、左側のシフトレジスタから個数を可変とするものが考えられる。なお、楕円曲線暗号化処理回路においては、シフトレジスタ群 5 0, 7 0 についても、同様に構成することができる。

【 0 0 8 7 】

このように、楕円曲線暗号化処理回路においては、3 組の 3 2 ビット幅のシフトレジスタ群 5 0, 6 0, 7 0 のそれぞれに対応して、ビット幅を可変とするためのバス切り替えスイッチ MUX 0, MUX 1, MUX 2 が設けられる。そこで、暗号化装置においては、回路規模の削減を図るために、上述したように、楕円曲線暗号化処理回路におけるシフトレジスタ群 5 0, 6 0, 7 0 と、SHA-1 処理回路におけるシフトレジスタとを共用するとともに、楕円曲線暗号化処理回

路におけるバス切り替えスイッチ MUX 0, MUX 1, MUX 2 と、SHA-1 処理回路におけるバス切り替えスイッチとを共用する。

【 0 0 8 8 】

さらに、上述した SHA-1 処理回路は、先に図 3 に示したように構成すると、32 ビット幅のシフトレジスタ群を用いて構成することができる。このような SHA-1 処理回路において、最終的な結果としてのハッシュ値や演算途中経過の値を保持するシフトレジスタは、先に図 2 に示したように、ALU RAM に代替することができる。したがって、暗号化装置においては、楕円曲線暗号化処理回路における演算処理で用いる図示しない ALU RAM と SHA-1 処理回路における ALU RAM とを共用する。これにより、暗号化装置においては、回路規模を抑制するのみならず、次回の楕円曲線暗号化処理にて用いるハッシュ値を ALU RAM に即座に格納することから、データ転送の手間を省略し、処理の高速化を図ることも可能となる。

【 0 0 8 9 】

また、楕円曲線暗号化処理回路にて算出された値や、SHA-1 処理回路における最終的な結果としてのハッシュ値や演算途中の値を ALU RAM に格納するために、楕円曲線暗号化処理回路や SHA-1 処理回路が ALU RAM にアクセスするに際しては、消費される電力が当該暗号化処理回路における他の各種信号処理において消費される電力のピークに比べてその電力のピークが大きい。そこで、後述するように、楕円曲線暗号化処理回路や SHA-1 処理回路が CPU や RAM からデータを受け取るに際してのゲートを制御し、ALU RAM へのアクセス以外の各種処理を制限することにより、ALU RAM へのアクセスと、他の各種処理とを時分割にて行い、該暗号化処理回路にて消費される消費電力のピークを低減することが可能となる。

【 0 0 9 0 】

また、楕円曲線暗号化処理回路や SHA-1 処理回路へのゲートが制限されるに際して、これら処理回路が CPU からの指示に関するデータを受け取ることなく処理を行うために、これら処理回路は自立的に処理を行うことができる。従って、該暗号化処理装置全体における瞬時電力を低減することができ、瞬時電力が

制限電力を超えた場合における再処理動作を行うことを低減することができ、処理を高速に行うことが可能となる。

【 0 0 9 1 】

最後に、D E S 暗号化処理を行うためのハードウェアであるD E S 暗号化処理回路について説明する。

【 0 0 9 2 】

D E S 暗号化処理回路は、D E S 暗号化処理を行うものである。D E S 暗号化とは、暗号化と復号とに同じ通信鍵を用いる共通鍵暗号化アルゴリズムの1つである。暗号化装置において、D E S 暗号化処理回路は、D E S 暗号化処理を3重に行ういわゆるトリプルD E S 暗号化処理を行うものとして構成される。

【 0 0 9 3 】

ここで、D E S 暗号化処理回路においては、トリプルD E S 暗号化処理を行うことから、通常のシングルD E S 暗号化処理を行う場合に比べ、鍵データを保持するシフトレジスタ群の規模が大きくなり、ビット列に対してD E S 暗号化処理を施す際の連鎖技法であるいわゆるC B C (Cipher Block Chaining) モードを行う際にも、シフトレジスタ群が必要となる。したがって、D E S 暗号化処理回路においては、これらのシフトレジスタ群をゲート換算すると、いわゆるSボックスに比較しても大きく、全体として回路規模を増大させる要因となる。

【 0 0 9 4 】

ところで、トリプルD E S 暗号化処理は、1つのD E S 演算処理コア回路を用いて、鍵データを3種類に変化させて3回演算処理を行うことによって実行される。そこで、D E S 暗号化処理回路としては、いわゆるT y p e A の非接触型I C カードに適用する場合には、先に図6に示した楕円曲線暗号化処理回路におけるシフトレジスタ群70を、この鍵データを保持するシフトレジスタ群として用いれば、楕円曲線暗号化処理回路に対する追加回路として、64ビット幅又は32ビット幅のバス切り替えスイッチを1つだけ設けるだけでよい。ここで、バス切り替えスイッチは、楕円曲線暗号化処理回路にも設けられていることから、D E S 暗号化処理回路としては、このバス切り替えスイッチを流用すれば追加回路も不要となる。一方、D E S 暗号化処理回路としては、いわゆるT y p e B

の非接触型 I C カードに適用する場合には、予め 3 種類の鍵データを用意しておき、シングル D E S 暗号化処理を行う毎に、2 個のシフトレジスタ分だけシフトして鍵データを交換することにより、T y p e A の場合と同様な動作を行うことができる。また、D E S 暗号化処理回路においては、データを保持するシフトレジスタや結果を保持するシフトレジスタについても、楕円曲線暗号化処理回路におけるシフトレジスタ群と共用することができることから、非常に僅かな追加回路でトリプル D E S 暗号化処理を行うことが可能となる。

【 0 0 9 5 】

このような D E S 暗号化処理回路は、具体的には、図 8 に示すように構成することができる。すなわち、D E S 暗号化処理回路は、図示しない C P U から供給されるデータを保持する 3 2 ビット幅のシフトレジスタ群 9 0 と、鍵データを保持するシフトレジスタ群 1 0 0 と、D E S 演算処理コア回路 1 2 0 を有する演算処理回路 1 1 0 とを備える。なお、同図における M U X , M U X 0 は、それぞれ、バス切り替えスイッチである。

【 0 0 9 6 】

D E S 暗号化処理回路においては、本来であれば 6 4 ビット幅のバッファを必要とするところ、3 2 ビット幅のシフトレジスタ群 9 0 , 1 0 0 でまかなうことができる。また、D E S 暗号化処理回路においては、トリプル D E S 暗号化処理に用いる鍵データの交換を行うためにバス切り替えスイッチを用いず、巡回させる形式とすることにより、バス切り替えスイッチを不要としている。このように、D E S 暗号化処理回路は、上述した楕円曲線暗号化処理回路に対して、D E S 演算処理コア回路 1 2 0 を含む演算処理回路 1 1 0 以外には殆ど追加回路を必要とせず、大幅に回路規模を削減することが可能となる。

【 0 0 9 7 】

さて、以上では、各部を共用しやすい構成とした S H A - 1 処理回路、楕円曲線暗号化処理回路、及び D E S 暗号化処理回路について説明したが、以下では、これらの S H A - 1 処理回路、楕円曲線暗号化処理回路、及び D E S 暗号化処理回路を統合して暗号化装置を構成することを考える。

【 0 0 9 8 】

先に図 2 に示した S H A - 1 処理回路、図 6 に示した楕円曲線暗号化処理回路、及び図 8 に示した D E S 暗号化処理回路を、それぞれ、重ね合わせると、共通の構成部位が極めて多く存在することがわかる。したがって、暗号化装置は、図 9 に示すように構成することができる。

【 0 0 9 9 】

すなわち、暗号化装置は、同図に示すように、2つのシフトレジスタ群 2 0 0 , 2 1 0 と、先に図 2 に示した S H A - 1 処理回路における R O M 3 0 に相当する R O M 2 2 0 と、先に図 2 に示した S H A - 1 処理回路における A L U R A M 4 0 及び先に図 6 に示した楕円曲線暗号化処理回路における楕円曲線演算処理コア回路 8 0 として機能するモンゴメリー演算回路 2 3 0 と、先に図 8 に示した D E S 暗号化処理回路における演算処理回路 1 1 0 に相当する演算処理回路 2 4 0 と、S H A - 1 処理における各種演算を行うための上述した各種演算処理回路とを備える。なお、同図においては、シフトレジスタ群 2 0 0 と演算処理回路 2 4 0 との配線については図示を省略している。

【 0 1 0 0 】

より具体的には、暗号化装置においては、先に図 2 に示した S H A - 1 処理回路におけるシフトレジスタ群 1 0 と、先に図 6 に示した楕円曲線暗号化処理回路におけるシフトレジスタ群 5 0 , 6 0 と、先に図 8 に示した D E S 暗号化処理回路におけるシフトレジスタ群 9 0 , 1 0 0 とを、シフトレジスタ群 2 0 0 として共用する。また、暗号化装置においては、先に図 2 に示した S H A - 1 処理回路におけるシフトレジスタ群 2 0 と、先に図 6 に示した楕円曲線暗号化処理回路におけるシフトレジスタ群 7 0 とを、シフトレジスタ群 2 1 0 として共用する。

【 0 1 0 1 】

さらに、暗号化装置においては、モンゴメリー演算回路 2 3 0 と S H A - 1 処理にて用いられる加算器とを、バス切り替えスイッチ M U X を介して接続することにより、楕円曲線暗号化処理にて用いられる加算器を削減している。

【 0 1 0 2 】

さらにまた、暗号化装置においては、先に図 2 に示した S H A - 1 処理回路におけるバス切り替えスイッチ M U X 0 と、先に図 6 に示した楕円曲線暗号化処理

回路におけるバス切り替えスイッチ MUX 0 と、先に図 8 に示した D E S 暗号化処理回路におけるバス切り替えスイッチ MUX 0 とを共用するとともに、先に図 6 に示した楕円曲線暗号化処理回路におけるバス切り替えスイッチ MUX 1 と、先に図 8 に示した D E S 暗号化処理回路におけるバス切り替えスイッチ MUX 0 とを共用する。

【 0 1 0 3 】

このように、暗号化装置においては、S H A - 1 処理回路、楕円曲線暗号化処理回路、及び D E S 暗号化処理回路における各部を共用することができ、後述する各処理モードに応じて動作させるハードウェアを時分割に切り替えることにより、本来必要とされるゲート数の約 1 / 2 程度のゲート数にまで回路規模を削減することができる。また、暗号化装置においては、回路規模の削減にともない、消費電力も約 1 / 2 程度にまで削減することができる。

【 0 1 0 4 】

さらに、後述する A L U R A M へのアクセスが行われるに際して、他の各種処理を制限することにより該暗号化処理装置全体で消費される電力の瞬時電力を低減することができる。特に、楕円暗号化処理回路や S H A - 1 処理回路にて演算された結果である値やハッシュ値を格納する A L U R A M へアクセスするに際しては、他の各種処理に比べて消費される瞬時電力が大きいことから、各種処理モードに応じて動作させるハードウェアを時分割で動作させることにより瞬時電力のピークを低減し、瞬時電力が制限電力を超えることによる再処理動作を行うことなく、高速な処理を可能とする。

【 0 1 0 5 】

さらに、暗号化装置においては、これらの各部を制御する図示しない C P U の負荷も削減することができる。例えば、暗号化装置においては、S H A - 1 処理によって算出されたハッシュ値の A L U R A M 上における格納場所を、楕円曲線暗号化処理にて用いられるアドレスに予め設定しておくことにより、S H A - 1 処理によるハッシュ値の算出後に、そのまま楕円曲線暗号化処理へと即座に移行することができることから、署名生成及び署名検証等の一連の動作の大半をハードウェアによって高速に実行することができる。したがって、暗号化装置にお

いては、CPUの負荷を削減することができ、さらには、ソフトウェアの改竄等による攻撃に対する耐性も強固となる。通常、暗号化処理においては、途中の演算結果の授受をCPUに委任した場合には、ソフトウェアを改竄することによって容易に成りすましを許容してしまう一方で、暗号化装置においては、このような演算途中におけるCPUの介入による改竄を回避することができる。

【0106】

さて、以下では、このような暗号化装置を適用した応用例について説明する。

【0107】

暗号化装置は、上述したように、非接触型ICカードに適用することができる。

【0108】

非接触ICカードは、例えば図10に示すように、各部を制御するCPU300と、このCPU300のワークエリアとして機能するメモリであって例えば2KB程度の容量を有するRAM310と、各種プログラム等を記憶する読み出し専用のメモリであって例えば32KB程度の容量を有するROM320と、電氣的に書き換え可能とされるメモリであって例えば9KB程度の容量を有するEEPROM (Electrically Erasable Programmable Read Only Memory) 330と、電源回路等のアナログブロック340と、無線通信を行うためのRF (Radio Frequency) ブロック350と、上述した楕円曲線暗号化処理、SHA-1処理、及びトリプルDES暗号化処理を行う暗号化装置に相当するECC/SHA1/DESブロック360と、例えば1KB程度の容量を有する上述したALURAM370と、テスター用のランドからなるテストブロック380と、CPU300と各部との間でデータの授受を行うためのバスであるCPUインターフェース390とを集積回路化したいわゆるLSI (Large Scale Integration) として構成される。

【0109】

このような非接触型ICカードは、先に図9に示した暗号化装置がECC/SHA1/DESブロック360として組み込まれたものである。非接触ICカードは、CPU300の制御のもとに、ECC/SHA1/DESブロック360

を動作させ、楕円曲線暗号化処理、SHA-1 処理、及びトリプルDES暗号化処理を行う。このとき、非接触型ICカードは、上述したように、各処理モードに応じて、動作させるハードウェアを時分割に切り替える。

【0110】

この時分割動作を具体的に説明するために、図11に示すように、各部を機能的に表現する。なお、同図においては、アナログブロック340については図示を省略するとともに、説明の便宜上、ECC/SHA1/DESブロック360を、楕円曲線暗号化処理及びSHA-1処理の機能を表すECC/SHA1ブロック360₁と、トリプルDES暗号化処理の機能を表すDESブロック360₂とに大別して表現している。

【0111】

このような非接触型ICカードにおける処理モードは、主に、通信を行う通信モード、楕円曲線暗号化処理を行う楕円曲線暗号化処理モード、トリプルDES暗号化処理を行うDES暗号化処理モード、及びALU RAM370に対してアクセスするALU RAMモードの4つに大別される。

【0112】

非接触型ICカードにおいては、通信モード時には、図12(A)中太線枠で示すように、CPU300、RAM310、ROM320、EEPROM330、及びRFブロック350が動作する。すなわち、非接触型ICカードにおいては、通信モード時には、CPU300の制御のもとに、ROM320に記憶されている所定の通信プログラムが起動し、RAM320やEEPROM330に記憶されている各種情報が、RFブロック350を介して外部に送信されるとともに、RFブロック350を介して外部から受信した各種情報が、RAM320やEEPROM330に記憶される。また、通信モード時には、暗号エンジンは各種処理を行うことがなく、該非接触型ICカード全体における消費電力は、通信モードで消費される電力に略等しくなる。つまり、通信モード、楕円曲線暗号化処理モード、トリプルDES暗号化処理モード、及びALU RAMモードを同時に動作させて各種処理を行うことがなく、通信モード時に消費される該非接触型ICカード全体における消費電力は、通信モードを動作させるに際して消費

される電力のみによって決まる。従って、該非接触型 I C カードにおける消費電力を低減することができるだけでなく、各モードを動作させるに際して消費される電力が同一時刻で加算される結果、該非接触型 I C カード全体における瞬時電力が制限電力を超えないように各種処理を行うことが可能となる。

【 0 1 1 3 】

また、非接触型 I C カードにおいては、楕円曲線暗号化処理モード時には、同図 (B) 中太線枠で示すように、ECC / SHA 1 ブロック 3 6 0 ₁ が動作する。すなわち、非接触型 I C カードにおいては、楕円曲線暗号化処理モード時には、ECC / SHA 1 ブロック 3 6 0 ₁ によって SHA - 1 処理が行われ、ハッシュ値を生成する。また、楕円曲線暗号化処理モード時には、CPU 3 0 0、RAM 3 1 0、ROM 3 2 0、EEPROM 3 3 0、及び RF ブロック 3 5 0 がアイドリング状態とされ、ECC / SHA 1 ブロック 3 6 0 ₁ から ALU RAM 3 7 0 へのハッシュ値の格納又は ALU RAM 3 7 0 からのハッシュ値の読み込みが制限される。

【 0 1 1 4 】

また、ECC / SHA 1 ブロック 3 6 0 ₁ は、楕円曲線暗号化処理モード時に CPU 3 0 0 から送られる処理に関する命令の如きアシストを受けることなく、自主的に処理を行うことができ、CPU 3 0 0、RAM 3 1 0、ROM 3 2 0、EEPROM 3 3 0、及び RF ブロック 3 5 0 による各種処理に対して時分割にて行うことが可能となる。従って、個別の処理における消費電力を低減することが可能となる。ECC / SHA 1 ブロック 3 6 0 ₁ と ALU RAM 3 7 0 との間における演算結果としてのハッシュ値の格納又は読み込みに際しては、ECC / SHA 1 ブロック 3 6 0 ₁ による演算処理中には、ALU RAM 3 7 0 との間におけるハッシュ値の受け渡しを行うことがなく、ECC / SHA 1 ブロック 3 6 0 ₁ の演算処理が一旦停止される。これにより、ECC / SHA 1 ブロック 3 6 0 ₁ における演算処理と、ALU RAM 3 7 0 へのアクセスが時分割で行われるように制限され、楕円曲線暗号化処理が行われる。

【 0 1 1 5 】

さらに、非接触型 I C カードにおいては、DES 暗号化処理モード時には、同

図 (C) 中太線枠で示すように、DES ブロック 3 6 0₂ が動作する。ここで、CPU 3 0 0、RAM 3 1 0、ROM 3 2 0 はアイドリング状態とされる。すなわち、非接触型 IC カードにおいては、DES 暗号化処理モード時には、DES ブロック 3 6 0₂ が、CPU 3 0 0 の制御のもとに、ROM 3 2 0 に記憶されている所定の擬似乱数 (Pseudo-random Number ; 以下、PN という。) 系列がシード (seed) や鍵データとして読み出され、RAM 3 1 0 がワークエリアとして用いられながら、DES ブロック 3 6 0₂ と、CPU 3 0 0、ROM 3 0 0 及び RAM 3 1 0 が時分割にて動作し、トリプル DES 暗号化処理が行われる。

【 0 1 1 6 】

さらに、非接触型 IC カードにおいては、ALU RAM モード時には、同図 (D) 中太線枠で示すように、ALU RAM 3 7 0 が動作し、ECC / SHA 1 ブロックが生成する演算結果及び ALU RAM 3 7 0 に格納されたデータを ALU RAM 3 7 0 と ECC / SHA 1 ブロック 3 6 0₁ との間で授受する。ALU RAM 3 7 0 を動作させるに際しては、CPU 3 0 0、RAM 3 1 0、ROM 3 2 0、EEPROM 3 3 0、及び RF ブロック 3 5 0 がアイドリング状態とされ、ECC / SHA 1 ブロック 3 6 0₁ とのデータの授受を制限し、消費電力を低減することができる。例えば、ECC / SHA 1 ブロック 3 6 0₁ を構成し、比較的消費電力が大きい乗算器から構成される回路にミュート回路を接続することにより、消費電力を低減することが可能となる。

【 0 1 1 7 】

図 1 3 は、縦軸を消費電力 W、横軸を処理時刻 T とし、これら各処理モードにおいて消費される消費電力を比較した図である。同図 (A) はゲートにおける消費電力、同図 (B) は ALU RAM における消費電力、同図 (C) は RAM における消費電力、さらに同図 (D) は、ECC / SHA 1 ブロックを構成するゲート、ALU RAM、及び RAM における消費電力を加算した該非接触型 IC カードにおける全体の消費電力を示す。同図 (A) に示すように、ゲートにおける消費電力は、処理回路を構成する乗算器などの処理に際しての遅延によりピークが抑制されるとともに処理時間に沿って分散することになる。これにより、ゲートで消費される消費電力のみに関して瞬時電力が抑制されることになる。

【0118】

さらに、同図（A）及び（B）に示すように、ALU RAMが処理回路にアクセスするに際してはゲートにおける処理が停止されることにより、ALU RAMで電力が消費されるタイミングにおいては、ゲートでは電力が消費されることがない。ALU RAMにおいて電力が消費される時刻 t_0 とゲートにおける電力が消費される時刻 t_1 とのタイミングがずれることにより、ゲートにおける消費電力とALU RAMにおける消費電力が同時に生じることがない。

【0119】

また、CPUやRAMから自立的に処理を行うことができることにより、ECC/SHA1ブロックとRAMとの間におけるデータの読み込みの回数を低減することができ、先に示した図14（C）に比べ、図13（C）に示すようにRAMにおける消費電力を低減することもできる。

【0120】

従って、図13（A）乃至（C）に示す各処理における消費電力を加算し、非接触型ICカードで消費される全体の消費電力は、同図（D）に示すように図14（D）に示す消費電力に比べて瞬時電力が低減されたものとすることができ、例えば、非接触型ICカードの制限電力が20mAである場合でも、制限電力を超えないように非接触型ICカードを動作させることが可能となる。

【0121】

このように、非接触型ICカードにおいては、比較的消費電力が大きい処理が行われるに際して、他の処理を制限することにより瞬時電力を低減することができ、制限電力を瞬時電力が超えることによる処理の遅延を生じることがなく高速な処理を行うことが可能となる。また、各処理モードに応じて、動作させるハードウェアを時分割に切り替えることにより、ハードウェアを共用した構成であっても、同時には行うことができない複数の処理を行うことが可能であるとともに、回路規模の削減と電力消費の削減とを図ることができる。

【0122】

以上説明したように、本発明の実施の形態として示す暗号化装置は、処理に際して瞬時電力が比較的大きいALU RAMへのアクセスに際して、他の各演算

処理を制限する。よって、他のECC／SHA1ブロックにおける処理のタイミングをずらすことにより瞬時電力を低減することができ、高速な処理を可能とすることができる。

【0123】

さらに、各種処理を行うための各ハードウェアを当該各種処理間で共用して時分割処理を行うことにより、回路規模を削減して極めて少ない電力消費のもとに高速且つ安全に公開鍵を用いた署名生成及び署名検証を行うこともできる。

【0124】

したがって、暗号化装置は、LSI等として実装する際に、チップサイズを大幅に小型化することができることから、非接触型ICカード等にも容易に適用することができる。このとき、暗号化装置は、電力消費が少なく済むことから、非接触型ICカードに適用した場合であっても、数センチメートルもの実用的な通信距離を実現することができ、該非接触型ICカードの動作時における消費電力が制限電力を超える度に再度処理をやり直すことなく、高速な処理を行うことが可能となる。また、暗号化装置は、改竄等の攻撃に対する耐性にも優れていることから、高い安全性が要求される非接触型ICカードを用いたサービスに適用して有効である。

【0125】

なお、本発明は、上述した実施の形態に限定されるものではない。例えば、上述した実施の形態では、公開鍵暗号化方式として、楕円曲線暗号化方式を採用して説明したが、本発明は、例えばRSA暗号化方式等の他の公開鍵暗号化方式にも容易に適用することができる。

【0126】

また、上述した実施の形態では、ハッシュ関数として、SHA-1を用いるものとして説明したが、本発明は、例えばMD5 (Message Digest 5) 等の他のハッシュ関数にも容易に適用することができる。

【0127】

さらに、上述した実施の形態では、暗号化処理を行う際に必要となる鍵生成の過程等において用いる乱数を、共通鍵暗号化方式の1つであるDES暗号化方式

を用いて生成するものとして説明したが、本発明は、乱数生成の手法については、任意のものを適用することができる。

【0128】

さらにまた、上述した実施の形態では、暗号化装置の適用例として、非接触型 I C カードを用いて説明したが、本発明は、同様の機能を要求する任意の装置やデバイスに適用することができるのは勿論である。

【0129】

このように、本発明は、その趣旨を逸脱しない範囲で適宜変更が可能であることとはいうまでもない。

【0130】

【発明の効果】

以上詳細に説明したように、本発明にかかる暗号化装置は、公開鍵暗号化方式による暗号化処理を行う暗号化装置であって、公開鍵暗号化方式による暗号化処理を行う公開鍵暗号化処理手段と、公開鍵暗号化処理手段によって用いるハッシュ値を生成するハッシュ値生成手段と、ハッシュ値を格納する記憶手段とを備え、少なくとも、ハッシュ値生成手段が記憶手段にアクセスするに際して、公開鍵暗号化処理手段における各種演算処理を制限する。

【0131】

したがって、本発明にかかる暗号化装置は、ハッシュ値を格納する A L U R A M へアクセスするに際して、他の各処理を停止することにより、暗号化装置における瞬時電力のピークを低減された状態のもとに、公開鍵を用いた署名生成及び署名検証を高速且つ安全に行うことができる。

【0132】

また、本発明にかかる暗号化装置は、公開鍵暗号化処理手段による暗号化処理とハッシュ値生成手段によるハッシュ値生成処理との間で、使用するレジスタ群を時分割共用することにより、回路規模を削減して極めて少ない電力消費のもとに公開鍵を用いた署名生成及び署名検証を安全に行うことができる。

【0133】

また、この本発明にかかる暗号化装置は、公開鍵暗号化処理手段によって暗号

化処理を行う際に必要となる乱数を生成するために、共通鍵暗号化方式による暗号化処理を行う共通鍵暗号化処理手段を備え、この共通鍵暗号化処理手段におけるデータを保持するレジスタ及び鍵データを保持するレジスタからなるレジスタ群を、公開鍵暗号化処理手段におけるレジスタ群と共用する。

【 0 1 3 4 】

したがって、本発明にかかる暗号化装置は、共通鍵暗号化処理手段を備える場合には、公開鍵暗号化処理手段による暗号化処理とハッシュ値生成手段によるハッシュ値生成処理との間のみならず、この共通鍵暗号化処理手段による暗号化処理との間でも、使用するレジスタ群を時分割共用することにより、より回路規模と電力消費とを削減することができる。

【 0 1 3 5 】

さらに、この本発明にかかる暗号化装置において、公開鍵暗号化処理手段は、公開鍵暗号化方式による暗号化処理に際する各種演算処理を行う公開鍵暗号化演算処理コア手段を有し、ハッシュ値生成手段は、ハッシュ値の生成処理に際する各種演算処理を行うハッシュ値演算処理コア手段を有し、公開鍵暗号化演算処理コア手段と、ハッシュ値演算処理コア手段とを共用する。

【 0 1 3 6 】

さらにまた、この本発明にかかる暗号化装置において、公開鍵暗号化処理手段は、ビット幅を可変とするためのバス切り替えスイッチを有し、ハッシュ値生成手段におけるバス切り替えスイッチを、公開鍵暗号化処理手段におけるバス切り替えスイッチと共用する。

【 0 1 3 7 】

したがって、本発明にかかる暗号化装置は、公開鍵暗号化処理手段による暗号化処理とハッシュ値生成手段によるハッシュ値生成処理との間で、演算処理に使用する演算処理コア手段を時分割共用し、また、公開鍵暗号化処理手段による暗号化処理とハッシュ値生成手段によるハッシュ値生成処理との間で、バス切り替えスイッチを時分割共用することにより、さらに大幅な回路規模の削減と電力消費の削減とを図ることができる。

【 0 1 3 8 】

また、この本発明にかかる暗号化装置は、公開鍵暗号化処理手段によって暗号化処理を行う際に必要となる乱数を生成するために、共通鍵暗号化方式による暗号化処理を行う共通鍵暗号化処理手段を備え、この共通鍵暗号化処理手段におけるバス切り替えスイッチを、公開鍵暗号化処理手段におけるバス切り替えスイッチと共用する。

【 0 1 3 9 】

したがって、本発明にかかる暗号化装置は、共通鍵暗号化処理手段を備える場合には、公開鍵暗号化処理手段による暗号化処理とハッシュ値生成手段によるハッシュ値生成処理との間のみならず、この共通鍵暗号化処理手段による暗号化処理との間でも、バス切り替えスイッチを時分割共用することにより、より回路規模と電力消費とを削減することができる。

【 0 1 4 0 】

さらに、この本発明にかかる暗号化装置は、ハッシュ値生成手段によって生成されたハッシュ値を格納する記憶手段を備え、ハッシュ値生成手段は、生成したハッシュ値を記憶手段に格納する際に、公開鍵暗号化処理手段によって用いられるアドレスに当該ハッシュ値を格納し、公開鍵暗号化処理手段は、記憶手段に格納されたハッシュ値を読み出す。

【 0 1 4 1 】

したがって、本発明にかかる暗号化装置は、ハッシュ値生成手段によって生成されたハッシュ値を、公開鍵暗号化処理手段による次回の暗号化処理にて用いるためにデータ転送することなく、記憶手段を介して受け渡すことにより、回路規模及び電力消費の削減のみならず、処理の高速化も図ることができる。

【図面の簡単な説明】

【図 1】 本発明の実施の形態として示す暗号化装置の概念を説明する図であって、(A) は、楕円曲線暗号化処理を行う暗号化エンジンにおけるハードウェア構成要素を機能分析的に分解した様子を示し、(B) は、SHA-1 処理を行う暗号化エンジンにおけるハードウェア構成要素を機能分析的に分解した様子を示し、(C) は、楕円曲線暗号化処理及び SHA-1 処理のそれぞれを行うためのハードウェア構成要素としてのレジスタを共用した様子を示す図である。

【図 2】 S H A - 1 処理回路の具体的な実装例としての構成を説明するブロック図である。

【図 3】 S H A - 1 処理回路の具体的な実装例としての他の構成を説明するブロック図である。

【図 4】 図 2 に示す S H A - 1 処理回路における基本動作を説明するためのフローチャートである。

【図 5】 図 2 に示す S H A - 1 処理回路における基本動作を説明するためのフローチャートであって、図 4 に示す工程に続く残りの工程を説明する図である。

【図 6】 楕円曲線暗号化処理回路の具体的な実装例としての構成を説明するブロック図である。

【図 7】 同楕円曲線暗号化処理回路の具体的な実装例としての要部構成を説明するブロック図であって、（A）は、シフトレジスタ群における各シフトレジスタのうち、右側のシフトレジスタから個数を可変としてビット幅を切り替える場合の構成を示し、（B）は、シフトレジスタ群における各シフトレジスタのうち、左側のシフトレジスタから個数を可変としてビット幅を切り替える場合の構成を示す図である。

【図 8】 D E S 暗号化処理回路の具体的な実装例としての構成を説明するブロック図である。

【図 9】 同暗号化装置の具体的な実装例としての構成を説明するブロック図である。

【図 1 0】 同暗号化装置を適用した非接触型 I C カードの構成を説明するブロック図である。

【図 1 1】 同非接触型 I C カードにおける各部を機能的に表現したブロック図である。

【図 1 2】 同非接触型 I C カードにおける時分割動作を説明するための図であり、（A）は、通信モード時における動作を説明するためのブロック図であり、（B）は、楕円曲線暗号化処理モード時における動作を説明するためのブロック図であり、（C）は、D E S 暗号化処理モード時における動作を説明するためのブロック図であり、（D）は、A L U R A M モード時における動作を説明する

ためのブロック図である。

【図 1 3】同非接触型 I C カードにおける消費電力を説明するための図であり、(A) は、ゲートにおける消費電力を説明する図であり、(B) は、A L U R A M アクセス時における消費電力を説明するための図であり、(C) は、R A M における消費電力を説明するための図であり、(D) は、該非接触型 I C カード全体の消費電力を説明するための図である。

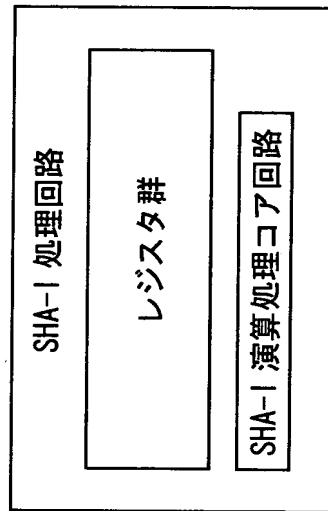
【図 1 4】従来の非接触型 I C カードにおける消費電力を説明するための図であり、(A) は、ゲートにおける消費電力を説明する図であり、(B) は、A L U R A M アクセス時における消費電力を説明するための図であり、(C) は、R A M における消費電力を説明するための図であり、(D) は、該非接触型 I C カード全体の消費電力を説明するための図である。

【符号の説明】

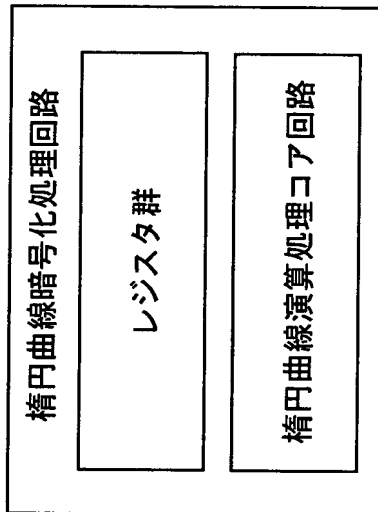
1 0, 2 0, 5 0, 6 0, 7 0, 9 0, 1 0 0, 2 0 0, 2 1 0 シフトレジスタ群、 3 0, 2 2 0, 3 2 0 R O M、 4 0, 3 7 0 A L U R A M、 8 0 楕円曲線演算処理コア回路、 1 1 0 演算処理回路、 1 2 0 D E S 演算処理コア回路、 2 3 0 モンゴメリー演算回路、 3 0 0 C P U、 3 1 0 R A M、 3 3 0 E E P R O M、 3 4 0 アナログブロック、 3 5 0 R F ブロック、 3 6 0 E C C / S H A 1 / D E S ブロック、 3 6 0₁ E C C / S H A 1 ブロック、 3 6 0₂ D E S ブロック、 3 8 0 テストブロック、 3 9 0 C P U インターフェース

【書類名】 図面

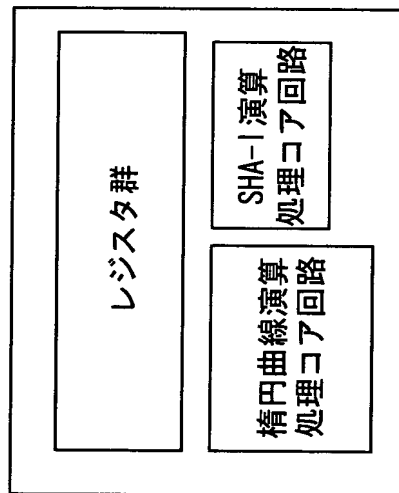
【図 1】



(B)



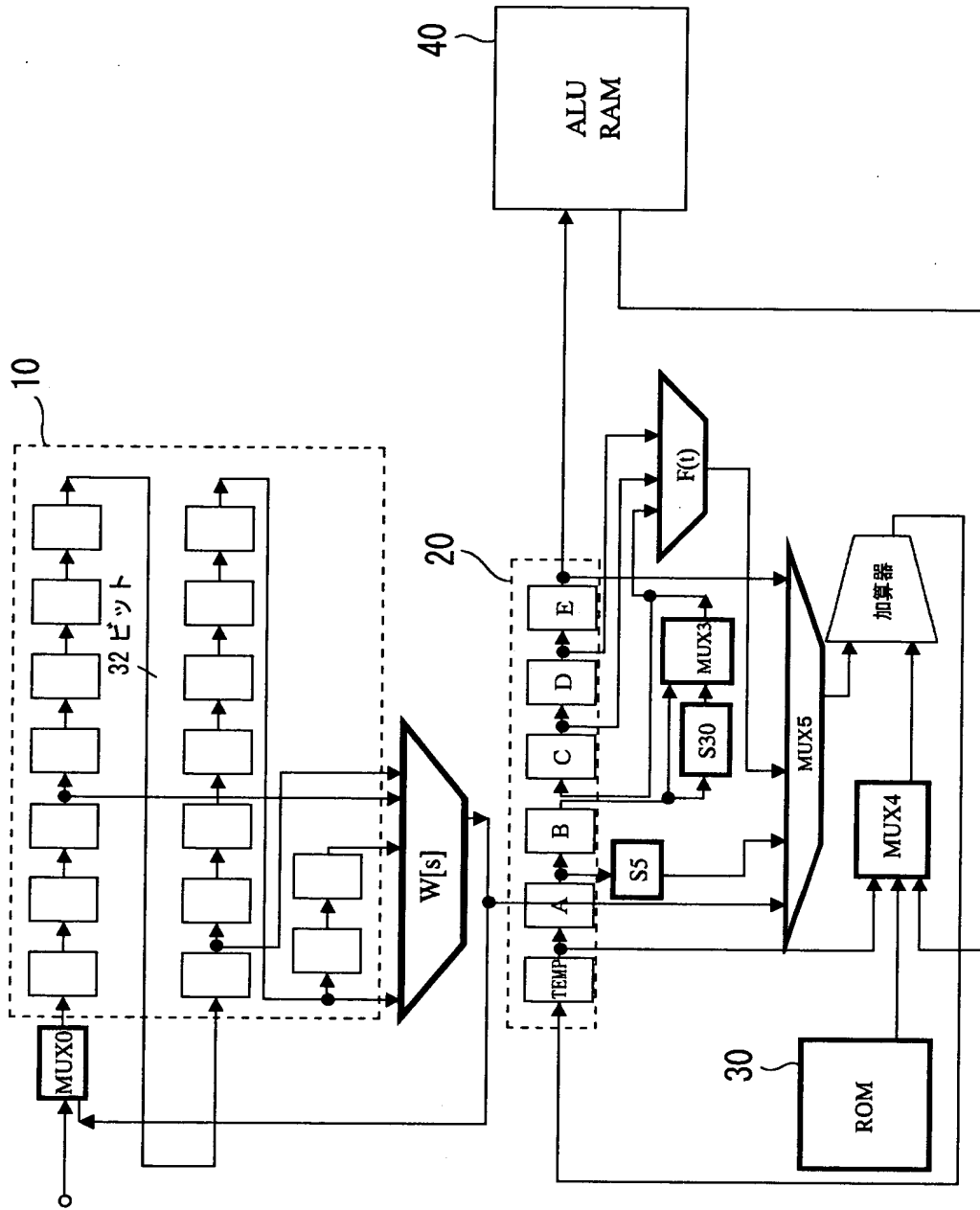
(A)



(C)

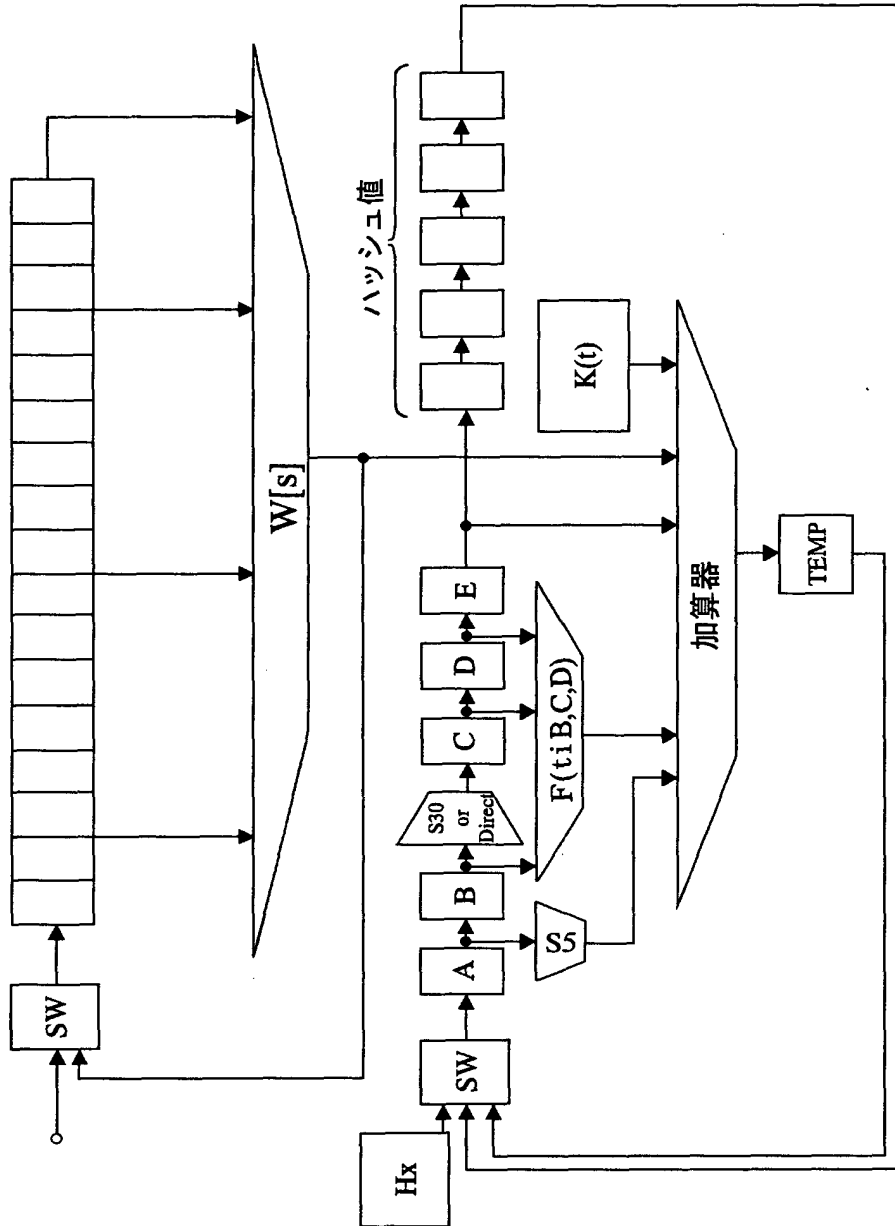
暗号化装置の概念図

【図 2】



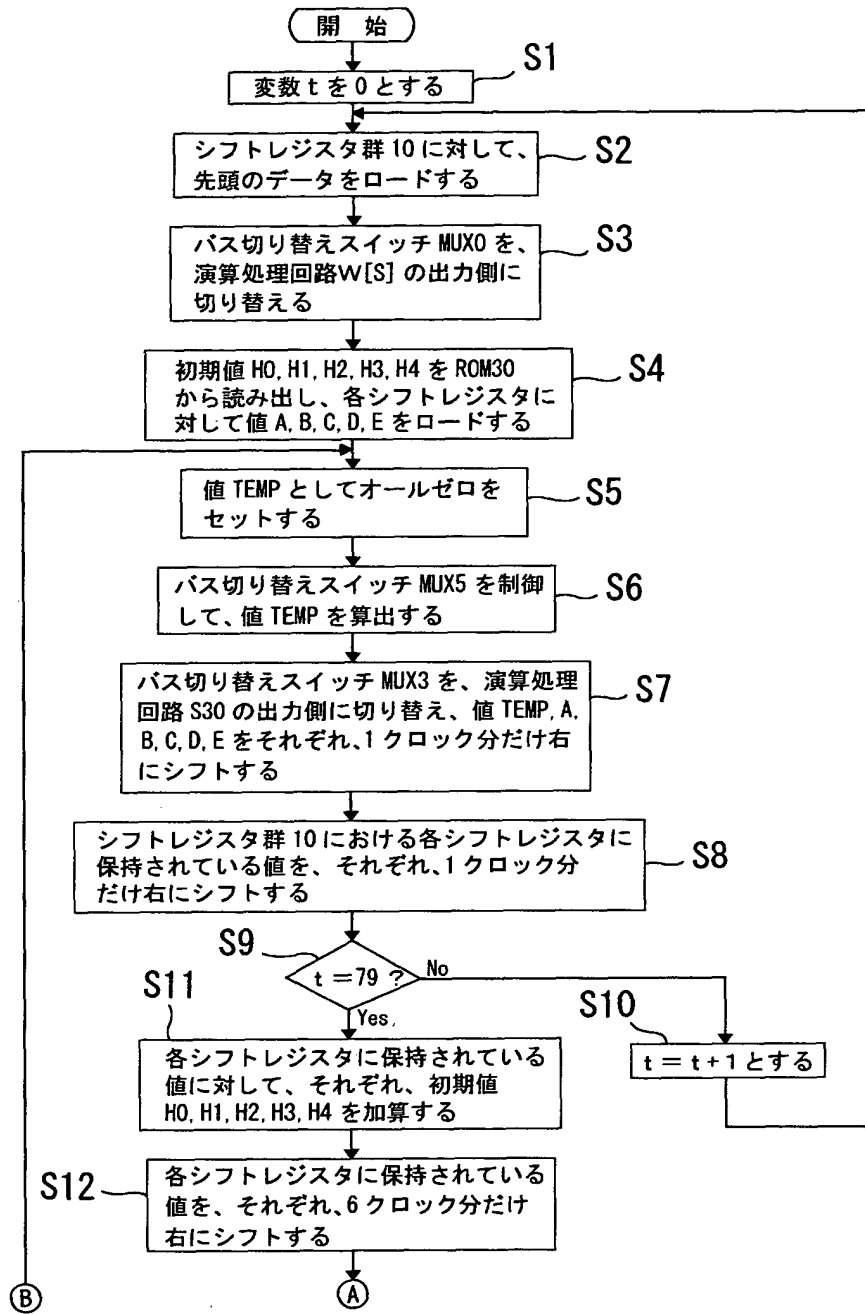
SHA-1 処理回路の構成ブロック図

【図 3】



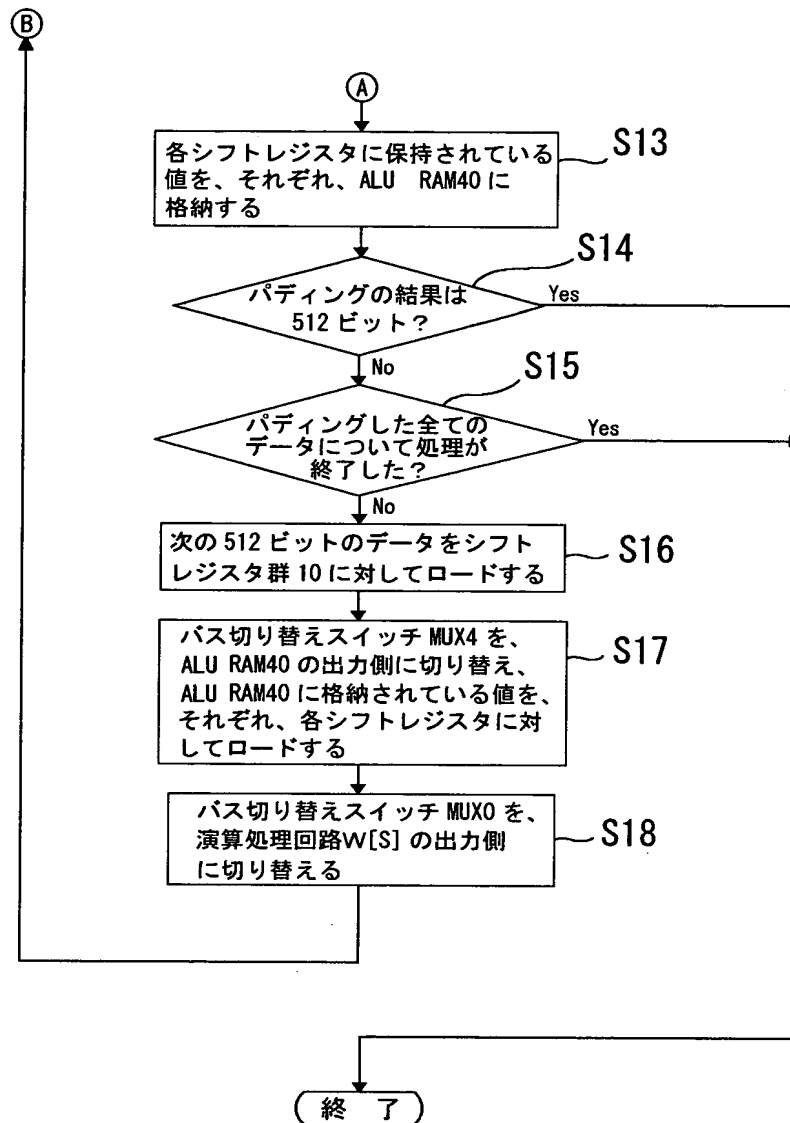
SHA-1 処理回路の構成ブロック図

【図4】



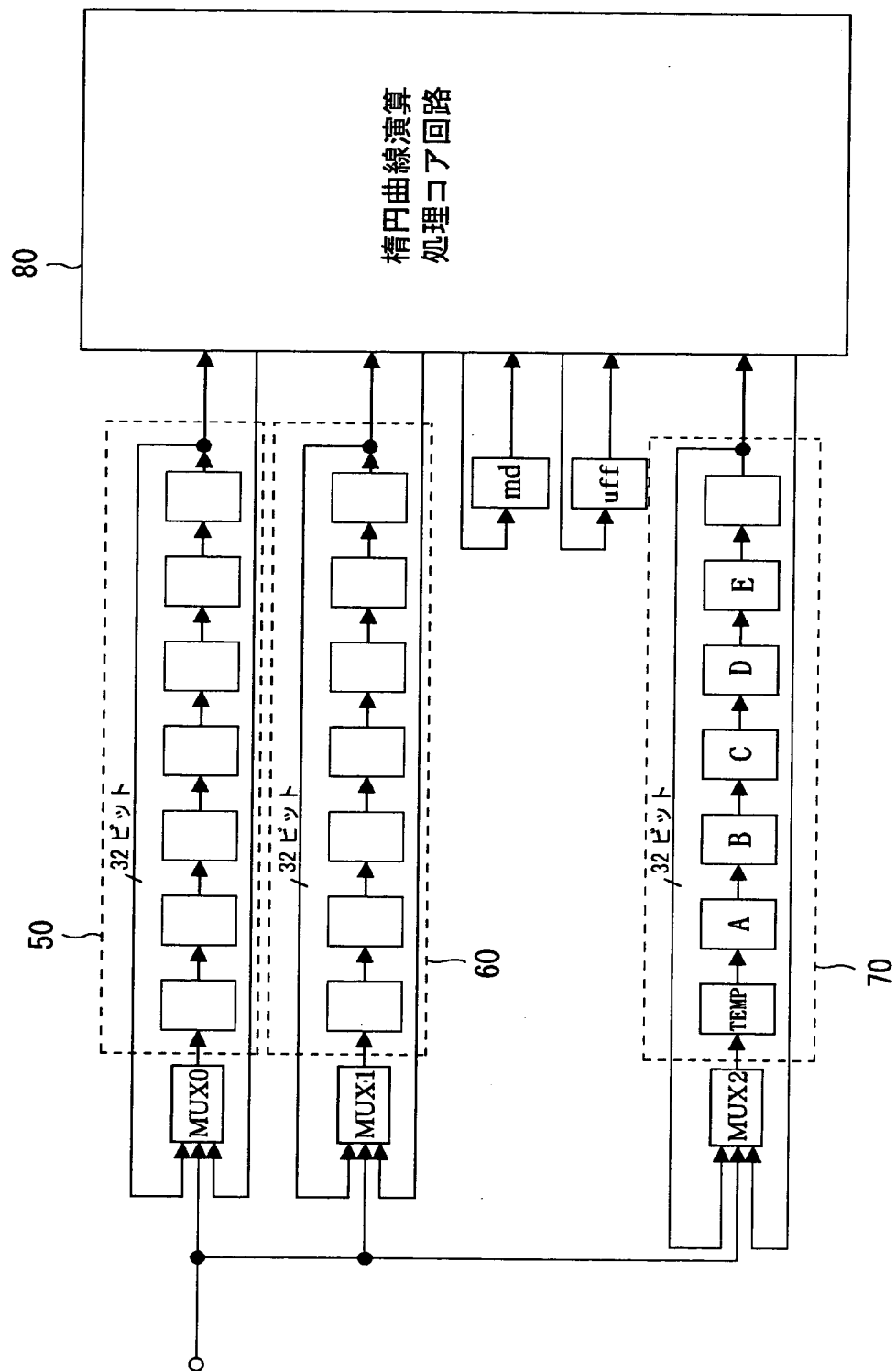
SHA-1 処理回路における一連の処理工程

【図 5】



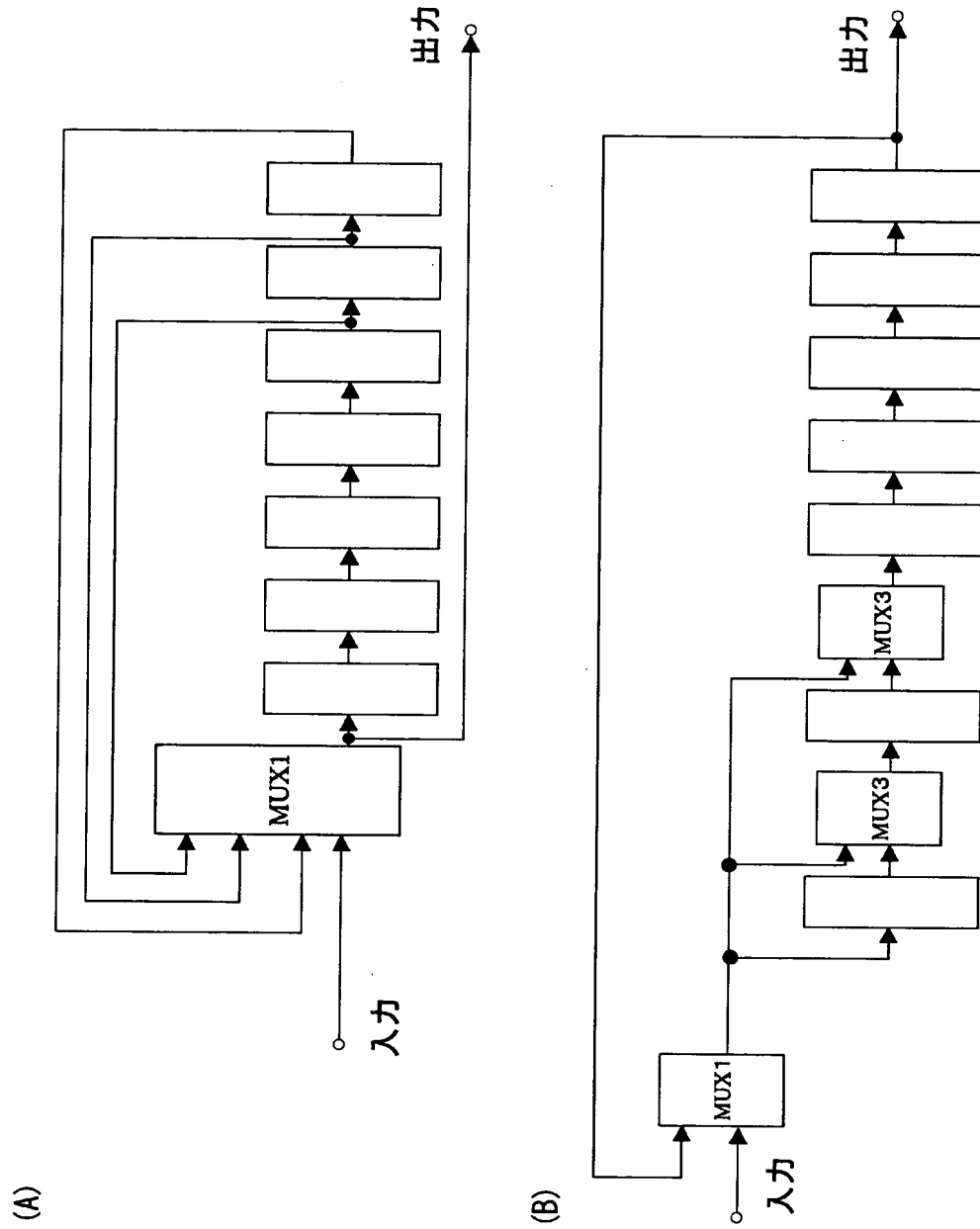
SHA-1 処理回路における一連の処理工程

【図6】



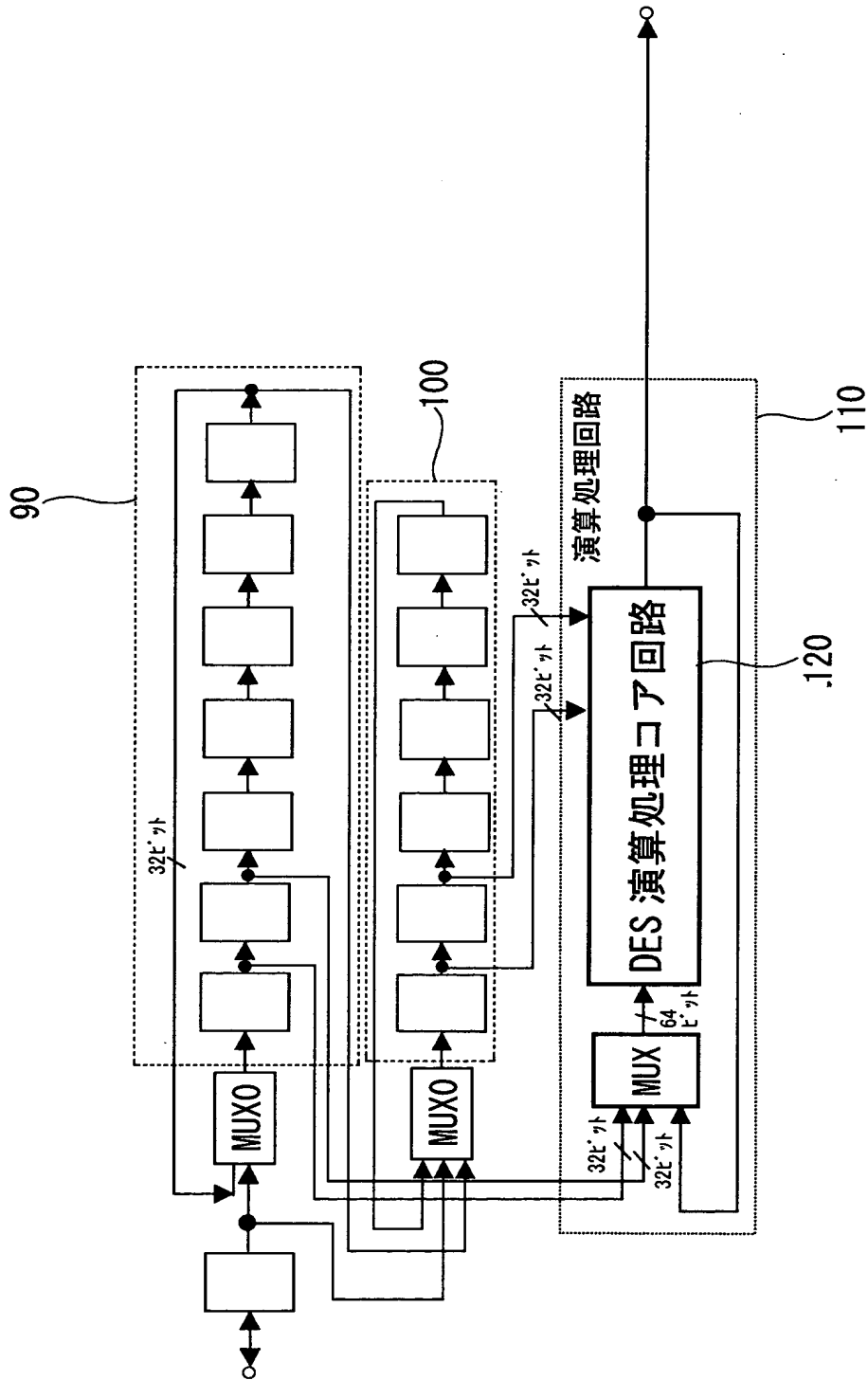
楕円曲線暗号化処理回路の構成ブロック図

【図 7】



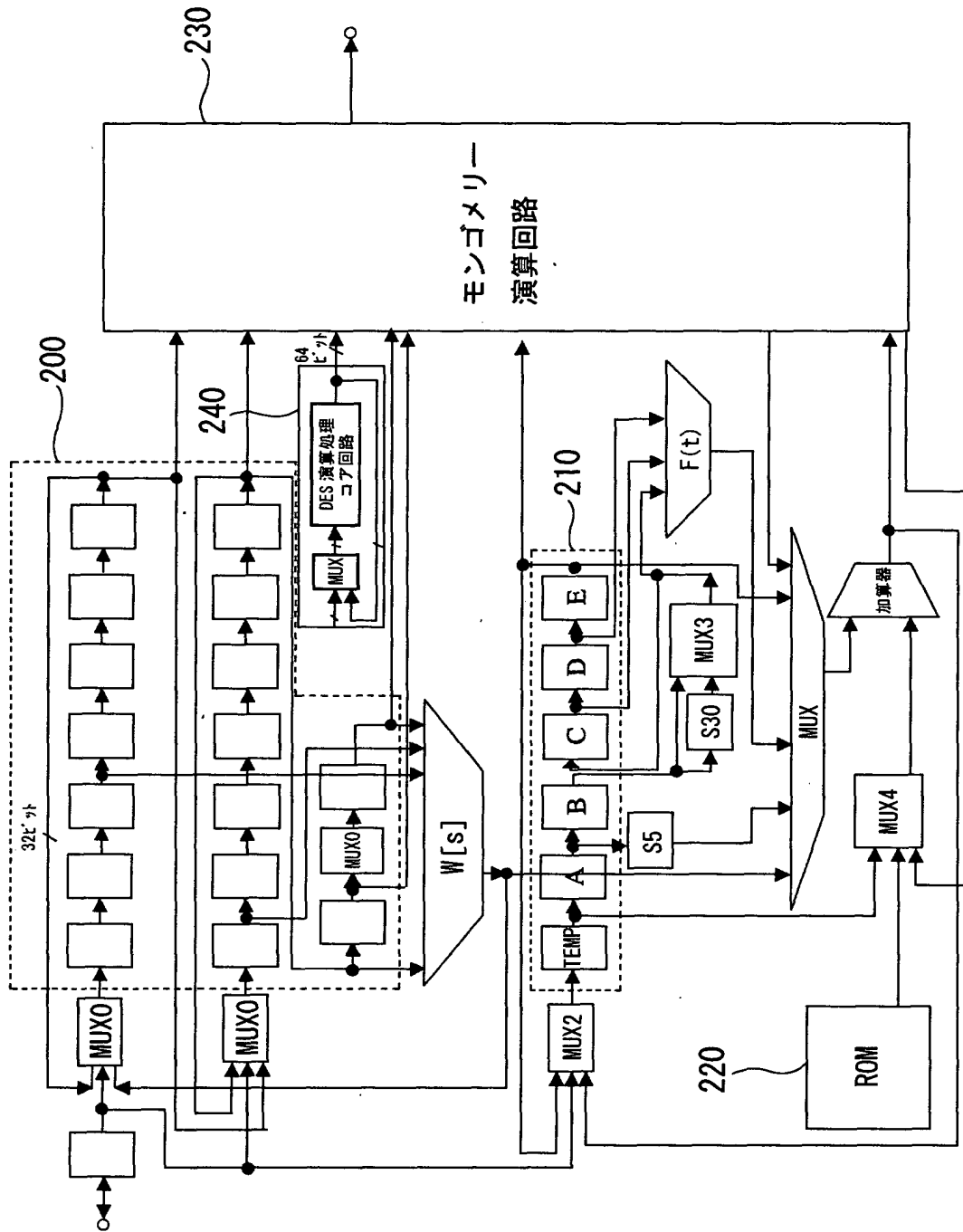
楕円曲線暗号化処理回路の要部構成ブロック図

【図 8】



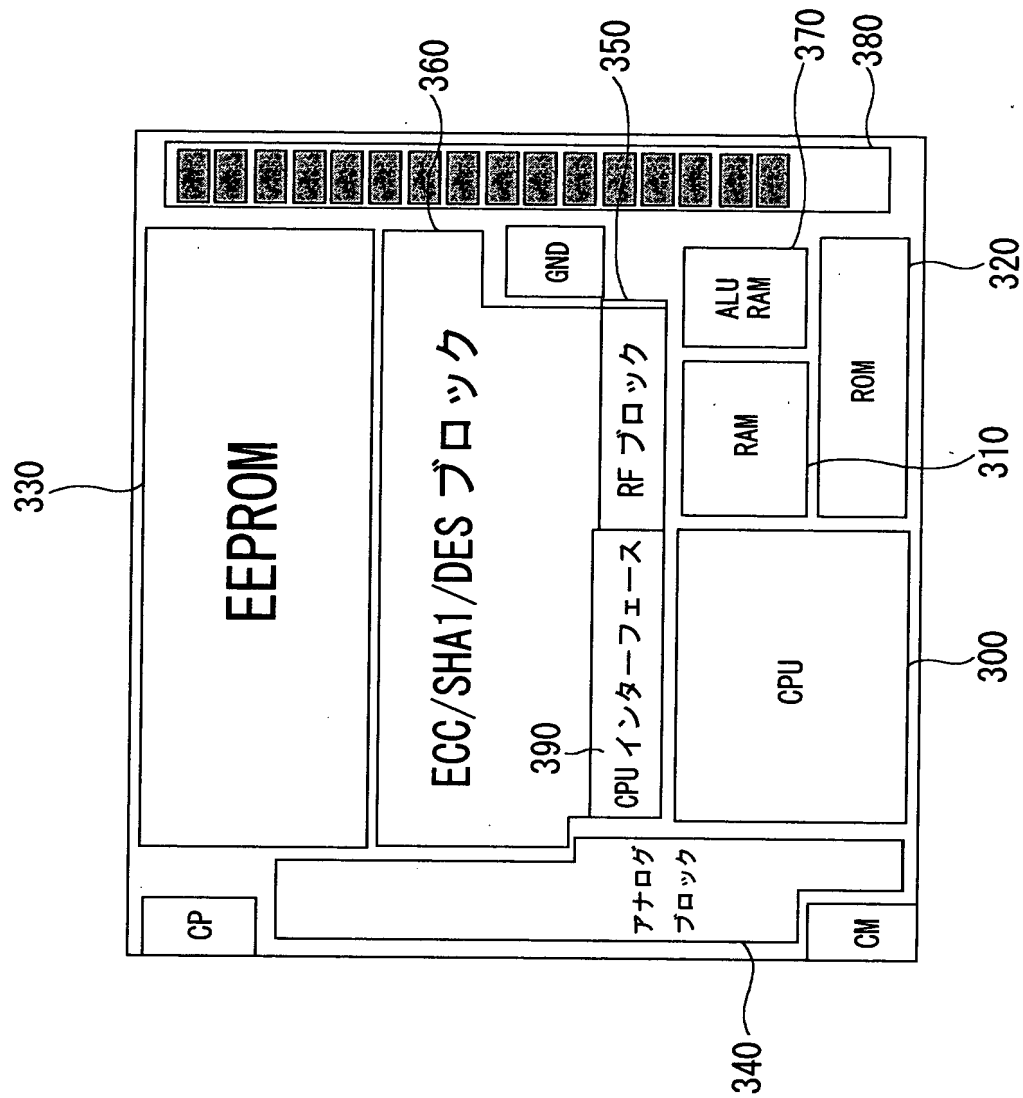
DES 暗号化処理回路の構成ブロック図

【図 9】



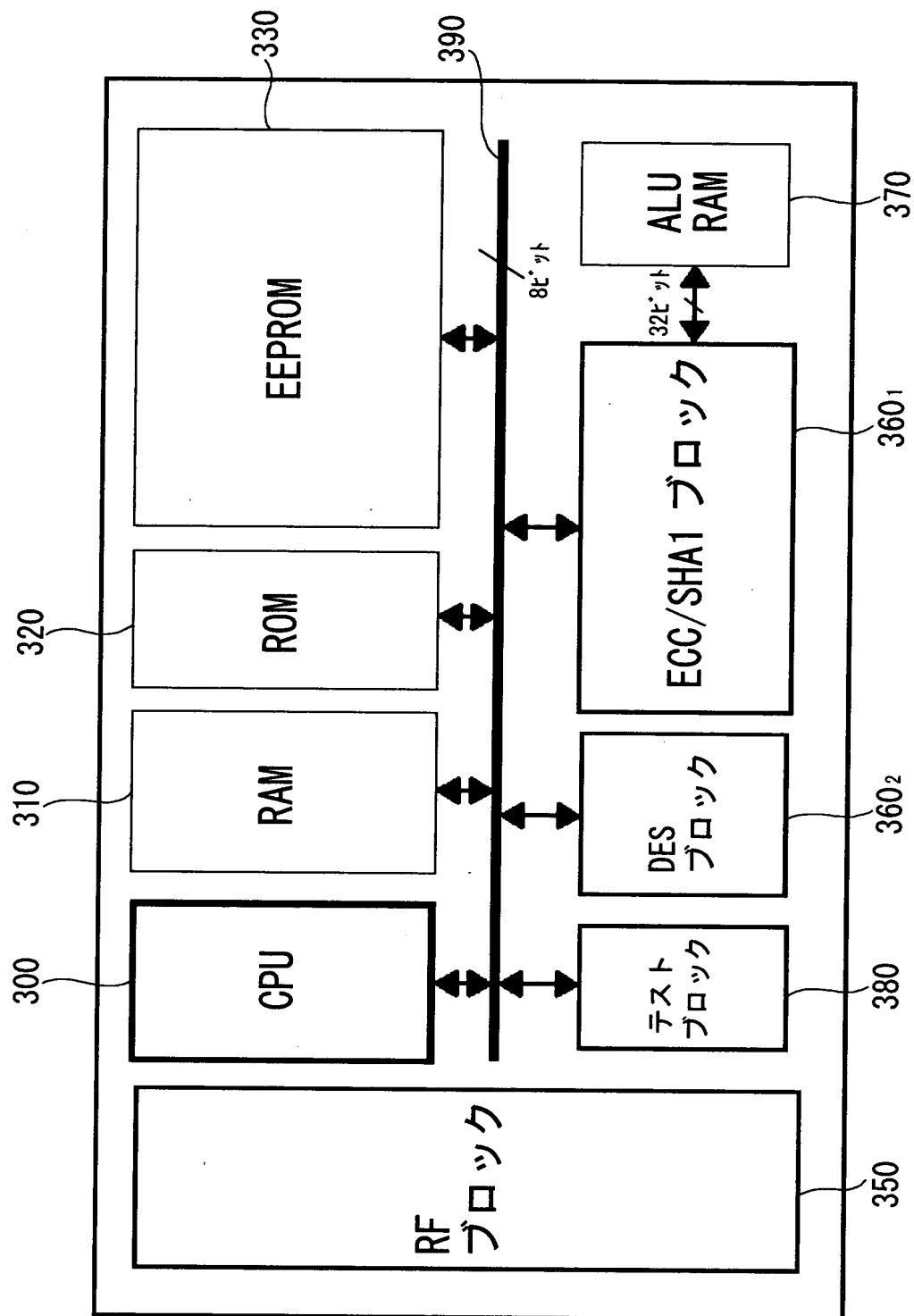
暗号化装置の構成ブロック図

【図10】



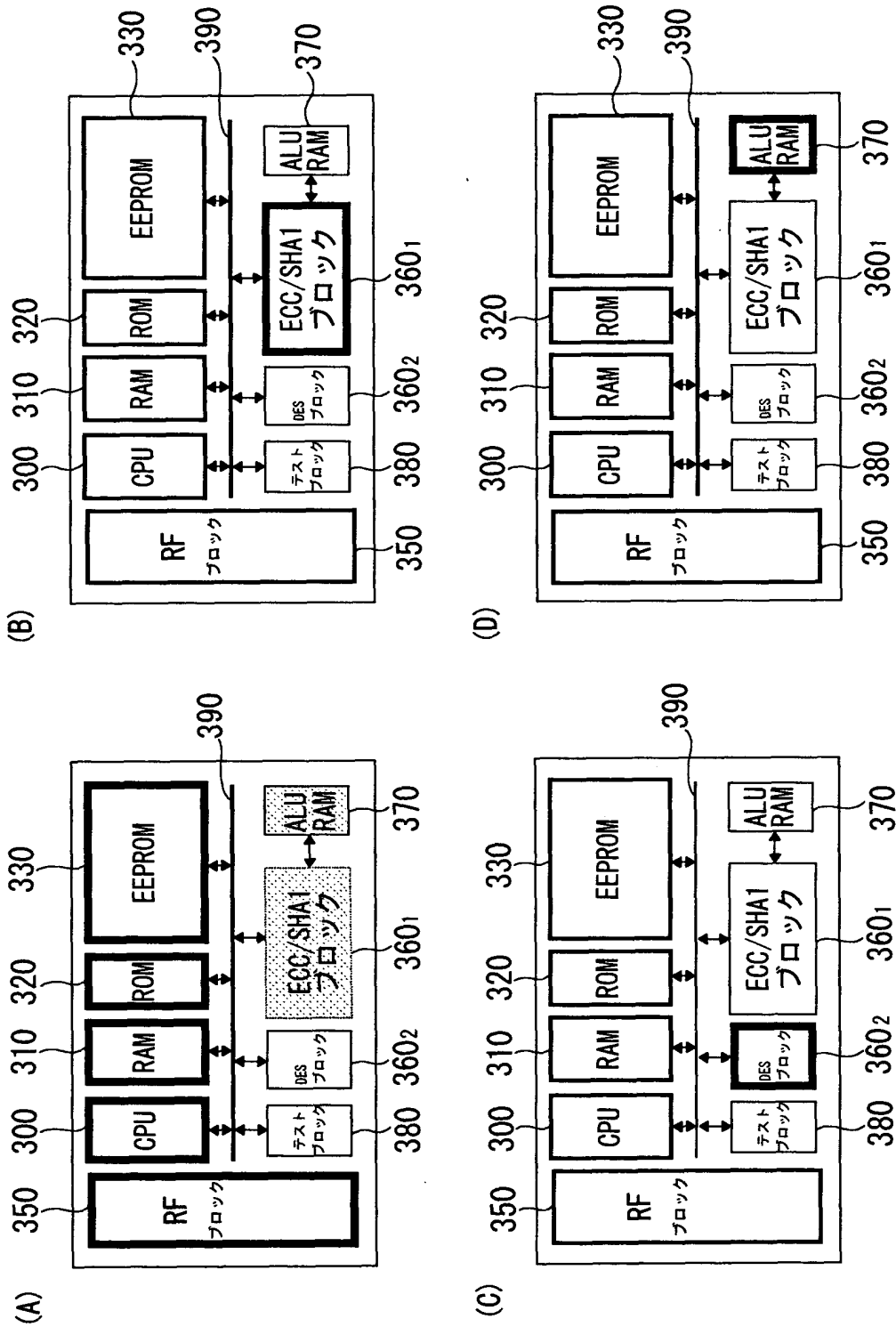
非接触型 IC カードの構成ブロック図

【図11】



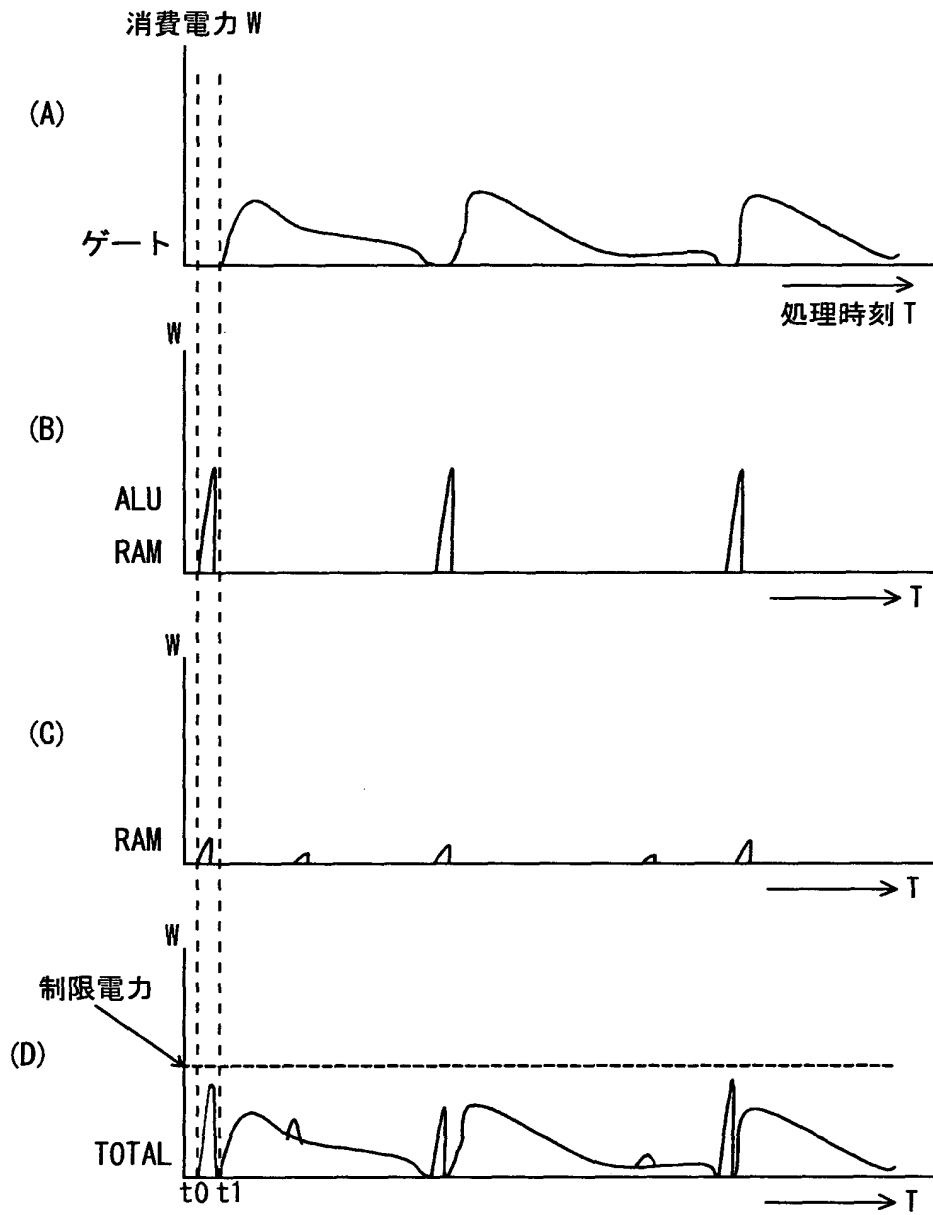
非接触型 IC カードの構成ブロック図

【図12】

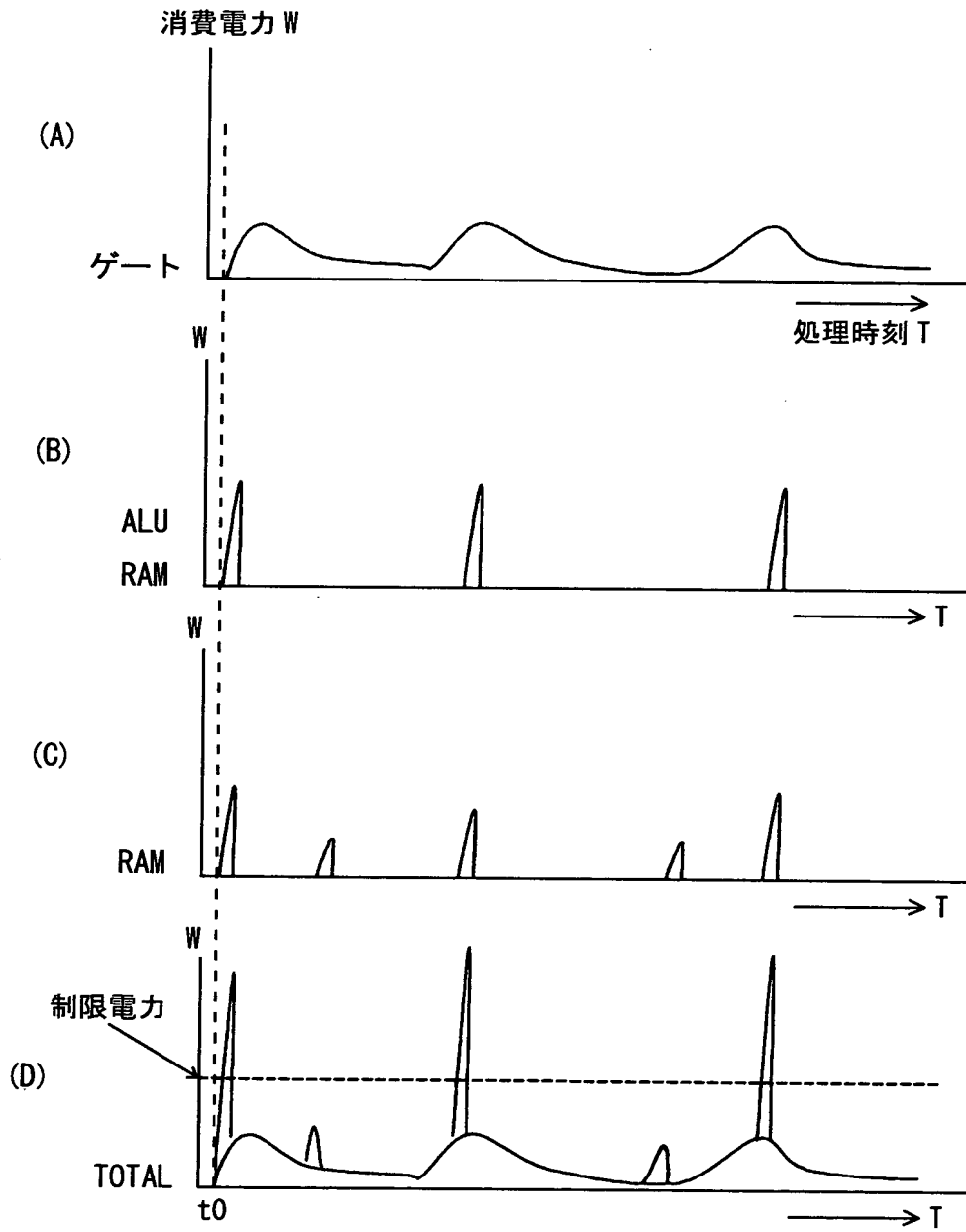


非接触型 IC カードの動作の説明図

【図 1 3】



【図 14】



【書類名】 要約書

【要約】

【課題】 瞬時電力を低減することにより高速且つ安全に公開鍵を用いた署名生成及び署名検証を可能とする暗号化装置を提供する。

【解決手段】 本発明にかかる暗号化装置は、公開鍵暗号化方式による暗号化処理を行う暗号化装置であって、公開鍵暗号化方式による暗号化処理を行う公開鍵暗号化処理手段と、公開鍵暗号化処理手段によって用いるハッシュ値を生成するハッシュ値生成手段と、ハッシュ値を格納する記憶手段とを備え、少なくとも、ハッシュ値生成手段が記憶手段にアクセスするに際して、公開鍵暗号化処理手段における各種演算処理を制限する。

【選択図】 図 1 2

出 願 人 履 歴 情 報

識別番号 [000002185]

1. 変更年月日 1990年 8月30日
[変更理由] 新規登録
住 所 東京都品川区北品川6丁目7番35号
氏 名 ソニー株式会社
2. 変更年月日 2003年 5月15日
[変更理由] 名称変更
住 所 東京都品川区北品川6丁目7番35号
氏 名 ソニー株式会社